

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Yingjiu Li (Ed.)

Data and Applications Security and Privacy XXV

25th Annual IFIP WG 11.3 Conference, DBSec 2011
Richmond, VA, USA, July 11-13, 2011
Proceedings



Springer

Volume Editor

Yingjiu Li
Singapore Management University (SMU)
School of Information Systems (SIS)
Room 80 04 049, 80 Stamford Road
Singapore 178902, Singapore
E-mail: yjli@smu.edu.sg

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-22347-1

e-ISBN 978-3-642-22348-8

DOI 10.1007/978-3-642-22348-8

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011930822

CR Subject Classification (1998): C.2, D.4.6, K.6.5, E.3, H.4, H.3

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

© IFIP International Federation for Information Processing 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at the 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy held in Richmond, Virginia, USA, July 11-13, 2011. This year's conference celebrated its 25th anniversary and presented the IFIP WG11.3 Outstanding Service Award and IFIP WG11.3 Outstanding Research Contribution Award for significant service contributions and outstanding research contributions, respectively, to the field of data and applications security and privacy.

The program of this year's conference consisted of 14 full papers and 9 short papers, which were selected from 37 submissions after rigorous review and intensive discussion by the Program Committee members and external reviewers. Each submission was reviewed by at least 3, and on average 3.9, Program Committee members or external reviewers. The topics of these papers include access control, privacy-preserving data applications, query and data privacy, authentication and secret sharing. The program also includes four invited papers.

The success of this conference was a result of the efforts of many people. I would like to thank the Organizing Committee members, including Peng Liu (General Chair), Meng Yu (General Co-chair), Adam J. Lee (Publicity Chair), Qijun Gu (Web Chair), Wanyu Zang (Local Arrangements Chair), and Vijay Atluri (IFIP WG 11.3 Chair), for their great effort in organizing this conference. I would also thank the Program Committee members and external reviewers for their hard work in reviewing and discussing papers.

Last but not least, my thanks go to the authors who submitted their papers to this conference and to all of the attendees of this conference. I hope you enjoy reading the proceedings.

July 2011

Yingjiu Li

Organization

Executive Committee

General Chair	Peng Liu, The Pennsylvania State University, USA
General Co-chair	Meng Yu, Virginia Commonwealth University, USA
Program Chair	Yingjiu Li, Singapore Management University, Singapore
Publicity Chair	Adam J. Lee, University of Pittsburgh, USA
Web Chair	Qijun Gu, Texas State University - San Marcos, USA
Local Arrangements Chair	Wanyu Zang, Virginia Commonwealth University, USA
IFIP WG 11.3 Chair	Vijay Atluri, Rutgers University, USA

Program Committee

Claudio Agostino Ardagna	Università degli Studi di Milano, Italy
Vijay Atluri	Rutgers University, USA
Kun Bai	IBM Research T.J. Watson, USA
Steve Barker	King's College, London University, UK
Joachim Biskup	Technische Universität Dortmund, Germany
Marina Blanton	University of Notre Dame, USA
David Chadwick	University of Kent, UK
Frédéric Cuppens	TELECOM Bretagne, France
Nora Cuppens-Bouahia	TELECOM Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Eduardo B. Fernandez	Florida Atlantic University, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Simon Foley	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Qijun Gu	Texas State University - San Marcos, USA
Ehud Gudes	Ben-Gurion University, Israel
Ragib Hasan	Johns Hopkins University, USA
Sokratis Katsikas	University of Piraeus, Greece

VIII Organization

Adam J. Lee	University of Pittsburgh, USA
Tieyan Li	Institute for Infocomm Research, Singapore
Yingjiu Li	Singapore Management University, Singapore
Peng Liu	The Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Emil Lupu	Imperial College, UK
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	Università di Bergamo, Italy
Wolter Pieters	University of Twente, The Netherlands
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Kui Ren	Illinois Institute of Technology, USA
Mark Ryan	University of Birmingham, UK
Kouchi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Anoop Singhal	NIST, USA
Traian Marius Truta	Northern Kentucky University, USA
Jaideep Vaidya	Rutgers University, USA
Hui Wang	Stevens Institute of Technology, USA
Lingyu Wang	Concordia University, Canada
Xiaokui Xiao	Nanyang Technological University, Singapore
Meng Yu	Virginia Commonwealth University, USA
Xinwen Zhang	Huawei Research Center, Santa Clara, California, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Zutao Zhu	Google Inc., USA

Additional Reviewers

Chan, Aldar	Nishide, Takashi
Chang, Katharine	Perez Martinez, Pablo Alejandro
Cheng, Pengsu	Pulls, Tobias
Erola, Arnau	Scalavino, Enrico
Hori, Yoshiaki	Soria Comas, Jordi
Iliadis, John	Su, Chunhua
Konstantinou, Elisavet	Van Cleeff, André
Kourai, Kenichi	Xiong, Huijun
Liu, Wen Ming	Xu, Wenjuan
Livraga, Giovanni	Zhang, Ge
Ma, Jiefei	Zhang, Yulong
Mohammed, Noman	Zhao, Bin

Table of Contents

Invited Papers

Information Flow Containment: A Practical Basis for Malware Defense	1
<i>R. Sekar</i>	
Re-designing the Web's Access Control System (Extended Abstract)	4
<i>Wenliang Du, Xi Tan, Tongbo Luo, Karthick Jayaraman, and Zutao Zhu</i>	
Integrated Management of Security Policies	12
<i>Stefano Paraboschi</i>	

Access Control I

Cooperative Data Access in Multi-cloud Environments	14
<i>Meixing Le, Krishna Kant, and Sushil Jajodia</i>	
Multiparty Authorization Framework for Data Sharing in Online Social Networks	29
<i>Hongxin Hu and Gail-Joon Ahn</i>	

Privacy-Preserving Data Applications I

Enforcing Confidentiality and Data Visibility Constraints: An OBDD Approach	44
<i>Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati</i>	
Public-Key Encrypted Bloom Filters with Applications to Supply Chain Integrity	60
<i>Florian Kerschbaum</i>	

Access Control II

An Optimization Model for the Extended Role Mining Problem	76
<i>Emre Uzun, Vijayalakshmi Atluri, Haibing Lu, and Jaideep Vaidya</i>	
Dynamics in Delegation and Revocation Schemes: A Logical Approach	90
<i>Guillaume Aucher, Steve Barker, Guido Boella, Valerio Genovese, and Leendert van der Torre</i>	

Data Confidentiality and Query Verification

History-Dependent Inference Control of Queries by Dynamic Policy
Adaption 106
Joachim Biskup

Multilevel Secure Data Stream Processing 122
Raman Adaikkalavan, Indrakshi Ray, and Xing Xie

Query and Data Privacy

Query Processing in Private Data Outsourcing Using Anonymization ... 138
Ahmet Erhan Nergiz and Chris Clifton

Private Database Search with Sublinear Query Time 154
Keith B. Frikken and Boyang Li

Privacy-Preserving Data Applications II

Efficient Distributed Linear Programming with Limited Disclosure 170
Yuan Hong, Jaideep Vaidya, and Haibing Lu

Privacy-Preserving Data Mining: A Game-Theoretic Approach..... 186
Atsuko Miyaji and Mohammad Shahriar Rahman

Authentication and Secret Sharing

Enhancing CardSpace Authentication Using a Mobile Device 201
Haitham S. Al-Sinani and Chris J. Mitchell

Verifiable Secret Sharing with Comprehensive and Efficient Public
Verification 217
Kun Peng

Short Papers

A Robust Remote User Authentication Scheme against Smart Card
Security Breach 231
Chun-Ta Li, Cheng-Chi Lee, Chen-Ju Liu, and Chin-Wen Lee

N-Gram Based Secure Similar Document Detection 239
Wei Jiang and Bharath K. Samanthula

An Index Structure for Private Data Outsourcing 247
Aaron Steele and Keith B. Frikken

Selective Disclosure on Encrypted Documents 255
Hao Lei and Dengguo Feng

A New Leakage-Resilient IBE Scheme in the Relative Leakage Model . . .	263
<i>Yu Chen, Song Luo, and Zhong Chen</i>	
Accurate Accident Reconstruction in VANET	271
<i>Yuliya Kopylova, Csilla Farkas, and Wenyuan Xu</i>	
Cyber Situation Awareness: Modeling the Security Analyst in a Cyber-Attack Scenario through Instance-Based Learning	280
<i>Varun Dutt, Young-Suk Ahn, and Cleotilde Gonzalez</i>	
Leveraging UML for Security Engineering and Enforcement in a Collaboration on Duty and Adaptive Workflow Model That Extends NIST RBAC	293
<i>Solomon Berhe, Steven Demurjian, Swapna Gokhale, Jaime Pavlich-Mariscal, and Rishi Saripalle</i>	
Preserving Privacy in Structural Neuroimages	301
<i>Nakeisha Schimke, Mary Kuehler, and John Hale</i>	
Author Index	309