

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, 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, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

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

For further volumes:

<http://www.springer.com/series/7410>

Joaquin Garcia-Alfaro · Georgios Lioudakis
Nora Cuppens-Boulahia · Simon Foley
William M. Fitzgerald (Eds.)

Data Privacy Management and Autonomous Spontaneous Security

8th International Workshop, DPM 2013, and
6th International Workshop, SETOP 2013
Egham, UK, September 12–13, 2013
Revised Selected Papers

Editors

Joaquin Garcia-Alfaro
Telecom SudParis
Evry
France

Georgios Lioudakis
National Technical University of Athens
Athens
Greece

Nora Cuppens-Boulahia
Telecom Bretagne
Cesson Sévigné
France

Simon Foley
University College Cork
Cork
Ireland

William M. Fitzgerald
IDA Ovens
EMC Information Systems International
Cork
Ireland

ISSN 0302-9743

ISBN 978-3-642-54567-2

DOI 10.1007/978-3-642-54568-9

Springer Heidelberg New York Dordrecht London

ISSN 1611-3349 (electronic)

ISBN 978-3-642-54568-9 (eBook)

Library of Congress Control Number: 2014934122

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

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

Foreword from the DPM 2013 Program Chairs

This volume contains the proceedings of the 8th Data Privacy Management International Workshop (DPM 2013), held in Egham, UK, at Royal Holloway, University of London, during September 12–13, 2013, in conjunction with the 18th annual European research event in Computer Security (ESORICS 2013) symposium. It includes a revised version of the papers selected for presentation at the workshop. Previous issues of the DPM workshop were held in 2012 in Pisa (Italy), 2011 in Leuven (Belgium), 2010 in Athens (Greece), 2009 in Saint Malo (France), 2007 in Istanbul (Turkey), 2006 in Atlanta (USA), and 2005 in Tokyo (Japan).

The aim of DPM is to promote and stimulate the international collaboration and research exchange on areas related to the management of privacy-sensitive information. This is a very critical and important issue for organizations and end-users. It poses several challenging problems, such as translation of high-level business goals into system level privacy policies, administration of sensitive identifiers, data integration and privacy engineering, among others.

In response to the call for participation, 46 submissions were received. Each submission was evaluated on the basis of significance, novelty, and technical quality. All submissions went through a careful anonymous review process (three or more reviews per submission) aided by 49 Technical Program Committee members and 31 additional referees. In the end, 13 full papers, accompanied by five short papers, were presented at the event. The final program also included three invited talks by Steven J. Murdoch (University of Cambridge), Emil Lupu (Imperial College London), and John Borking (former Privacy Commissioner and Board Member of the Dutch Data Protection Authority in The Hague). Our special thanks to Steven, Emil, and John for accepting our invitation and for their presence during the event and talks.

We would like to thank everyone who helped at organizing the event, including all the members of the Organizing Committee of both ESORICS and DPM 2013. In particular, we would like to highlight and acknowledge the tremendous efforts of the ESORICS 2013 General Chair Keith Mayes and his team. Thank you Keith for all your help and support with DPM. Our gratitude goes also to Pierangela Samarati, Steering Committee Chair of the ESORICS Symposium, for all her arrangements to make possible the satellite events. Our special thanks to the General Chairs of DPM 2013, Josep Domingo-Ferrer and Maryline Laurent, as well as Steering Committee member Guillermo Navarro-Arribas, for their unconditional help since the beginning of this event. Last but by no means least, we thank all the DPM 2013 Program Committee members, additional reviewers, all the authors who submitted papers, and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsors of the workshop: Institute Mines-Telecom, CNRS Samovar UMR 5157, Telecom SudParis, UNESCO Chair in Data Privacy, and National Technical University of Athens.

8th International Workshop on Data Privacy Management—DPM 2013

Program Committee Chairs

Joaquin Garcia-Alfaro	Telecom SudParis, France
Georgios Lioudakis	National Technical University of Athens, Greece

Workshop General Chairs

Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Maryline Laurent	Telecom SudParis, France

Program Committee

Esma Aimeur	Université de Montreal, Canada
Michel Barbeau	Carleton University, Canada
John Borking	Borking Consultancy, The Netherlands
Jens-Matthias Bohli	NEC Laboratories Europe, Germany
Ana Cavalli	Telecom SudParis, France
Frederic Cuppens	Telecom Bretagne, France
Nora Cuppens-Boulahia	Telecom Bretagne, France
Roberto Di Pietro	Roma Tre University of Rome, Italy
Nicola Dragoni	Technical University of Denmark, Denmark
Christian Duncan	Quinnipiac University, USA
David Evans	University of Derby, UK
Sara Foresti	Università degli Studi di Milano, Italy
Sebastien Gambs	University of Rennes 1, France
Flavio D. Garcia	Radboud University Nijmegen, The Netherlands
Paolo Gasti	New York Institute of Technology, USA
Francesca Gaudino	Baker & McKenzie Law Firm, Italy
Stefanos Gritzalis	University of the Aegean, Greece
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz, Germany
Artur Hecker	Telecom ParisTech, France
Jordi Herrera	Autonomous University of Barcelona, Spain
Iakovos Venieris	National Technical University of Athens, Greece
Dimitra Kaklamani	National Technical University of Athens, Greece
Panos Kampanakis	Cisco Systems, USA
Georgia Kapitsaki	University of Cyprus, Cyprus

Sokratis Katsikas	University of Piraeus, Greece
Evangelos Kranakis	Carleton University, Canada
Jean Leneutre	Telecom ParisTech, France
Giovanni Livraga	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Brad Malin	Vanderbilt University, USA
Sotirios Maniatis	Hellenic Authority for Communications Privacy, Greece
Chris Mitchell	Royal Holloway, UK
Refik Molva	Eurecom, France
Krish Muralidhar	University of Kentucky, USA
Guillermo Navarro-Arribas	Autonomous University of Barcelona, Spain
Silvio Ranise	Fondazione Bruno Kessler, Italy
Kai Rannenber	Goethe University Frankfurt, Germany
Indrajit Ray	Colorado State University, USA
Yves Roudier	Eurecom, France
Mark Ryan	University of Birmingham, UK
Claudio Soriente	ETH Zürich, Switzerland
Alessandro Sorniotti	IBM Research, Switzerland
Traian M. Truta	Northern Kentucky University, USA
Yasuyuki Tsukada	NTT Communication Science Laboratories, Japan
Jens Weber	University of Victoria, Canada
Lena Wiese	University of Göttingen, Germany
Yanjiang Yang	Institute for Infocomm Research, Singapore
Nicola Zannone	Eindhoven University of Technology, The Netherlands
Melek Önen	Eurecom, France

Steering Committee

Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Joaquin Garcia-Alfaro	Telecom SudParis, France
Guillermo Navarro-Arribas	Autonomous University of Barcelona, Spain
Vicenç Torra	Artificial Intelligence Research Institute, Spain

Additional Reviewers

Achilleas Achilleos	Christian Kahl
Ahmad Sabouri	David Galindo
Alessio Di Mauro	David Nuñez
Ana Nieto	Elisa Costante
Anderson Morais	Eugenia Papagiannakopoulou
Anis Bkakria	Fatbardh Veseli
Aouadi Mohamed	Flavio Lombardi

Gurchetan S. Grewal	Monir Azraoui
Ian Batten	Montserrat Batet
Jia Liu	Sara Hajian
Jiangshan Yu	Sebastiaan De Hoogh
Jose Luis Vivas	Sokratis Vavilis
Kaoutar Elkhyaoui	Tarik Moataz
Khalifa Toumi	Vasilios Katos
Maria Karyda	Xiaoping Che
Maria Koukovini	

Foreword from the SETOP 2013 Program Chairs

These are the proceedings of the 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013).

The purpose of this workshop is to bring together researchers to explore challenges in the automated configuration of security. In this volume you will find papers on a range of topics related to authentication and authorization, mobile security and vulnerabilities.

The workshop program also included invited talks by Steven Murdoch (University of Cambridge, UK) on “Quantifying and Measuring Anonymity” and by Emil Lupu (Imperial College London) on “Pervasive Autonomous Systems: Challenges in Policy based Adaptation and Security.”

As with previous years, SETOP was a satellite workshop of the European Symposium on Research in Computer Security (ESORICS). We are grateful to the ESORICS 2013 Organizing Committee for agreeing to host SETOP-2013 and especially to ESORICS General Chair Keith Mayes for his assistance and support.

We are grateful to the many people who contributed to the success of the workshop. The members of the Program Committee and external reviewers. The Publications Chair, William Fitzgerald assembled the workshops proceedings and ensured its timely publication.

Finally, the workshops would not be possible without the authors who submitted papers, the presenters, and attendees.

We hope you enjoy reading the proceedings.

Nora Cuppens-Boulahia
Simon Foley

6th International Workshop on Autonomous and Spontaneous Security—SETOP 2013

Program Committee Chairs

Research Track

Simon Foley University College Cork, Ireland
Nora Cuppens-Boulahia Telecom Bretagne, France

Industrial Track

Edgardo Montes de Oca Montimage, France

Workshop General Chairs

Ana Cavalli Telecom SudParis, France
Frédéric Cuppens Telecom Bretagne, France

Publicity and Publication Chair

William Fitzgerald University College Cork, Ireland

Webmaster

Said Oulmakhzoune Telecom Bretagne, France

Program Committee

Fabien Autrel	Telecom Bretagne, France
Gildas Avoine	Catholic University of Louvain, Belgium
Michele Bezzi	SAP Research, France
Christophe Bidan	Supelec, France
Carlo Blundo	University of Salerno, Italy
Joan Borrell-Viader	UAB, Spain
Jordi Castella-Roca	Rovira i Virgili University, Spain
Iliano Cervesato	Carnegie Mellon University, Qatar
Stelvio Cimato	Università degli Studi di Milano, Italy
Mauro Conti	Università di Padova, Italy
Ernesto Damiani	Università degli Studi di Milan, Italy
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy

Josep Domingo-Ferrer	Rovira i Virgili University, Spain
William Fitzgerald	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Jerome Francois	University of Luxembourg, Luxembourg
Joaquin Garcia-Alfaro	Telecom SudParis, France
Stefanos Gritzalis	University of the Aegean, Greece
Olivier Heen	Technicolor, France
Wei Jiang	Missouri University of S&T, USA
Sokratis Katsikas	University of Piraeus, Greece
Florian Kerschbaum	SAP Research, France
Evangelos Kranakis	Carleton University, Canada
Marie Noelle Lepareux	Thales, France
Javier Lopez	University of Malaga, Spain
Giovanni Livraga	Università degli Studi di Milano, Italy
Wissam Mallouli	Montimage, France
Guillermo Navarro-Arribas	Autonomous University of Barcelona, Spain
Marie Nuadi	EADS-Cassidian, France
Andreas Pashalidis	K.U. Leuven, Belgium
Nicolas Prigent	Supélec, France
Yves Roudier	Eurecom, France
Thierry Sans	Carnegie Mellon University, Qatar
George Spanoudakis	City University London, UK
Radu State	University of Luxembourg, Luxembourg
Ari Takanen	Codenomicon, Finland
Bachar Wahbi	Percevio, France

Steering Committee

Ana-Rosa Cavalli	Telecom SudParis, France
Frédéric Cuppens	Telecom Bretagne, France
Nora Cuppens-Boulahia	Telecom Bretagne, France
Jean Leneutre	Telecom ParisTech, France
Yves Roudier	Eurecom, France

Contents

Keynote Address

Quantifying and Measuring Anonymity	3
<i>Steven J. Murdoch</i>	

Data Privacy Management

Performance Evaluation of Primitives for Privacy-Enhancing Cryptography on Current Smart-Cards and Smart-Phones	17
<i>Jan Hajny, Lukas Malina, Zdenek Martinasek, and Ondrej Tethal</i>	
Practical Packing Method in Somewhat Homomorphic Encryption	34
<i>Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshihara</i>	
Collaborative and Privacy-Aware Sensing for Observing Urban Movement Patterns	51
<i>Nelson Gonçalves, Rui José, and Carlos Baquero</i>	
Parallel Implementation of GC-Based MPC Protocols in the Semi-Honest Setting	66
<i>Mauro Barni, Massimo Bernaschi, Riccardo Lazzeretti, Tommaso Pignata, and Alessandro Sabellico</i>	
Privacy Analysis of a Hidden Friendship Protocol	83
<i>Florian Kammüller and Sören Preibusch</i>	
Anonymous and Transferable Electronic Ticketing Scheme	100
<i>Arnau Vives-Guasch, M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Jordi Castellà-Roca, and Josep-Lluís Ferrer-Gomila</i>	
Privacy-Preserving Publish/Subscribe: Efficient Protocols in a Distributed Model	114
<i>Giovanni Di Crescenzo, Brian Coan, John Schultz, Simon Tsang, and Rebecca N. Wright</i>	
Privacy-Preserving Processing of Raw Genomic Data	133
<i>Erman Ayday, Jean Louis Raisaro, Urs Hengartner, Adam Molyneaux, and Jean-Pierre Hubaux</i>	
Using Search Results to Microaggregate Query Logs Semantically.	148
<i>Arnau Erola and Jordi Castellà-Roca</i>	

Legal Issues About Metadata Data Privacy vs Information Security	162
<i>Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy, and Magali Ricarde</i>	
Privacy-Preserving Multi-Party Reconciliation Secure in the Malicious Model . . .	178
<i>Georg Neugebauer, Lucas Brutschy, Ulrike Meyer, and Susanne Wetzel</i>	
Differentially Private Smart Metering with Battery Recharging	194
<i>Michael Backes and Sebastian Meiser</i>	
AppGuard – Fine-Grained Policy Enforcement for Untrusted Android Applications.	213
<i>Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky</i>	
Autonomous and Spontaneous Security	
Reference Monitors for Security and Interoperability in OAuth 2.0.	235
<i>Ronan-Alexandre Cherrueau, Rémi Douence, Jean-Claude Royer, Mario Südholt, Anderson Santana de Oliveira, Yves Roudier, and Matteo Dell’Amico</i>	
Remote Biometrics for Robust Persistent Authentication	250
<i>Mads I. Ingwar and Christian D. Jensen</i>	
Classifying Android Malware through Subgraph Mining	268
<i>Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra</i>	
Introducing Probabilities in Contract-Based Approaches for Mobile Application Security	284
<i>Gianluca Dini, Fabio Martinelli, Ilaria Matteucci, Andrea Saracino, and Daniele Sgandurra</i>	
Advanced Detection Tool for PDF Threats	300
<i>Quentin Jerome, Samuel Marchal, Radu State, and Thomas Engel</i>	
Enforcing Input Validation through Aspect Oriented Programming.	316
<i>Gabriel Serme, Theodoor Scholte, and Anderson Santana de Oliveira</i>	
Lightweight Cryptography for Embedded Systems – A Comparative Analysis	333
<i>Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos</i>	
Short Papers	
A Simulation of Document Detection Methods and Reducing False Positives for Private Stream Searching	353
<i>Michael Oehler and Dhananjay S. Phatak</i>	

Dynamic Anonymous Index for Confidential Data	362
<i>Guillermo Navarro-Arribas, Daniel Abril, and Vicenç Torra</i>	
Are On-Line Personae Really Unlinkable?	369
<i>Meilof Veeningen, Antonio Piepoli, and Nicola Zannone</i>	
On the Privacy of Private Browsing – A Forensic Approach	380
<i>Kiavash Satvat, Matthew Forshaw, Feng Hao, and Ehsan Toreini</i>	
Privacy-Preserving Trust Management Mechanisms from Private Matching Schemes	390
<i>Oriol Farràs, Josep Domingo-Ferrer, and Alberto Blanco-Justicia</i>	
Author Index	399