

*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*

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*

Vijay Atluri Günther Pernul (Eds.)

# Data and Applications Security and Privacy XXVIII

28th Annual IFIP WG 11.3 Working Conference, DBSec 2014  
Vienna, Austria, July 14-16, 2014  
Proceedings



Springer

## Volume Editors

Vijay Atluri  
Rutgers University  
1 Washington Park, Newark, NJ 07102, USA  
E-mail: atluri@rutgers.edu

Günther Pernul  
Universität Regensburg  
Universitätsstraße 31, 93053 Regensburg, Germany  
E-mail: guenther.pernul@wiwi.uni-regensburg.de

ISSN 0302-9743  
ISBN 978-3-662-43935-7  
DOI 10.1007/978-3-662-43936-4  
Springer Heidelberg New York Dordrecht London

e-ISSN 1611-3349  
e-ISBN 978-3-662-43936-4

Library of Congress Control Number: 2014941798

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

© IFIP International Federation for Information Processing 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.

*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 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC) held in Vienna, Austria, July 14–16, 2014. This year's conference continued its tradition of being a forum for disseminating original research results and practical experiences in data and applications security and privacy.

This year we had an excellent program that consisted of 8 regular research paper sessions with 22 regular research papers, and 4 short papers, which were selected from a total of 63 submissions after a rigorous reviewing process by the Program Committee members and external reviewers. These sessions included such topics as access control, privacy, networked and mobile environments, data access, cloud databases and private retrieval. In addition, the program included two keynote talks by Chris Clifton and Reinhard Posch.

The success of this conference was a result of the efforts of many people. We would like to extend our appreciation to the Program Committee members and external reviewers for their hard work. We would like to thank the general chairs, Pierangela Samarati, and Edgar Weippl, for taking care of the organization aspects of the conference. We would also like to thank Yvonne Poul for serving as the local arrangement chair and for promptly updating the conference web page, and Giovanni Livraga for serving as the publication chair. Special thanks go to Alfred Hofmann, Editorial Director of Springer, for agreeing to include these conference proceedings in the Lecture Notes in Computer Science series.

Last but not least, my thanks go to all of the authors who submitted papers and to all of the attendees. We hope you find the program stimulating and beneficial for your research. Welcome and enjoy the conference.

July 2014

Vijay Atluri  
Günther Pernul

# Organization

## Program Committee

Gail-Joon Ahn	Arizona State University, USA
Claudio Agostino Ardagna	Universita' degli Studi di Milano, Italy
Vijay Atluri	Rutgers University, USA
Joachim Biskup	Technische Universität Dortmund, Germany
Marina Blanton	University of Notre Dame, USA
David Chadwick	University of Kent, UK
Soon Ae Chun	CUNY, USA
Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Sabrina De Capitani Di Vimercati	Universita' degli Studi di Milano, Italy
Mourad Debbabi	Concordia University, Canada
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Eduardo B. Fernandez	Florida Atlantic University, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Sara Foresti	Universita' degli Studi di Milano, Italy
Ehud Gudes	Ben-Gurion University, Israel
Ragib Hasan	University of Alabama at Birmingham, USA
Yuan Hong	University at Albany, SUNY, USA
Sushil Jajodia	George Mason University, USA
Sokratis Katsikas	University of Piraeus, Greece
Adam J. Lee	University of Pittsburgh, USA
Haibing Lu	Santa Clara University, USA
Emil Lupu	Imperial College, UK
Martin Olivier	ICSA, University of Pretoria, South Africa
Sylvia Osborn	The University of Western Ontario, Canada
Stefano Paraboschi	Universita di Bergamo, Italy
Guenther Pernul	
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Kui Ren	State University of New York at Buffalo, USA
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Universita' degli Studi di Milano, Italy
Andreas Schaad	SAP AG, Germany
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Heechang Shin	Iona College, USA
Shamik Sural	IIT, Kharagpur, India

## VIII Organization

Traian Marius Truta  
Jaideep Vaidya  
Lingyu Wang  
Meng Yu  
Zutao Zhu

Northern Kentucky University, USA  
Rutgers University, USA  
Concordia University, Canada  
Virginia Commonwealth University, USA  
Google Inc., USA

## Additional Reviewers

Alrabae, Saed  
Blanco-Justicia, Alberto  
Boukhtouta, Amine  
Centonze, Paolina  
Gaspar, Jaime  
Hahn, Florian  
Hang, Isabelle  
Haque, Md  
Huo, Wei  
Jarraya, Yosr  
Jhanwar, Mahabir Prasad  
Kawamoto, Junpei  
Khalili, Mina  
Khan, Rasib  
Le, Meixing  
Livraga, Giovanni  
Madi, Leila  
Matsumoto, Shinichi  
Moataz, Tarik  
Mueller, Tobias

Mukherjee, Subhojeet  
Mulamba, Dieudonne  
Ohtaki, Yasuhiro  
Preda, Stere  
Pujol, Marta  
Ray, Sujoy  
Romero, Cristina  
Rufian-Torrell, Guillem  
Sabaté-Pla, Albert  
Servos, Daniel  
Sgandurra, Daniele  
Shirani, Paria  
Soeanu, Andrei  
Sun, Kun  
Wang, Guan  
Zang, Wanyu  
Zawoad, Shams  
Zhang, Lei  
Zhang, Mengyuan  
Zhang, Yihua

## **Abstracts of Invited Talks**

# Privacy without Encrypting: Protect Your Data and Use It Too

Chris Clifton

Purdue University, West Lafayette, IN 47907, USA  
clifton@cs.purdue.edu  
<http://www.cs.purdue.edu/people/clifton>

There has been ongoing work in encrypted database as a means to protect privacy, but this comes at a high price. An alternative is separating sensitive and identifying information, through models such as fragmentation[2], anatomization[6], and slicing[3]. In our DBSec'11 paper, we presented a query processor over such a data separation model, where the server cannot violate privacy constraints, but still does most of the work before sending final results to be joined by the client (who is allowed access to private data.)[4] A follow-on paper extended this to updates.[5] In DBSec'13 we showed how to ensure privacy constraints are satisfied when storing transactional data under such a model.[1]

This talk will look at using such data: How do we learn (and what can't we learn) when data is stored under a data separation approach. This involves both server-only approaches (what value can the server get in return for storing privacy-protected data), and client/server cooperation (pushing as much work to the server as possible, with the client doing only what is needed to ensure quality results.) We will look at anonymization techniques that support learning while providing privacy, as well as data mining techniques adapted to this model.

This talk presents work that was made possible by NPRP grant 02-256-1-046 from the Qatar National Research Fund. The statements made herein are solely the responsibility of the author.

## References

1. Al Bouna, B., Clifton, C., Malluhi, Q.: Using safety constraint for transactional dataset anonymization. In: Wang, L., Shafiq, B. (eds.) DBSec 2013. LNCS, vol. 7964, pp. 164–178. Springer, Heidelberg (2013)
2. Ciriani, V., Vimercati, S.D.C.D., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Combining fragmentation and encryption to protect privacy in data storage. *ACM Trans. Inf. Syst. Secur.* 13, 22:1–22:33 (2010), <http://doi.acm.org/10.1145/1805974.1805978>
3. Li, T., Li, N., Zhang, J., Molloy, I.: Slicing: A new approach for privacy preserving data publishing. *IEEE Transactions on Knowledge and Data Engineering* 24(3), 561–574 (2012), <http://doi.ieeecomputersociety.org/10.1109/TKDE.2010.236>



4. Nergiz, A.E., Clifton, C.: Query processing in private data outsourcing using anonymization. In: Li, Y. (ed.) DBSec. LNCS, vol. 6818, pp. 138–153. Springer, Heidelberg (2011)
5. Nergiz, A.E., Clifton, C., Malluhi, Q.: Updating outsourced anatomized private databases. In: 16th International Conference on Extending Database Technology (EDBT), Genoa, Italy, March 18-22, pp. 179–190 (2013), <http://doi.acm.org/10.1145/2452376.2452399>
6. Xiao, X., Tao, Y.: Anatomy: Simple and effective privacy preservation. In: Proceedings of 32nd International Conference on Very Large Data Bases (VLDB 2006), Seoul, Korea, September 12-15 (2006), <http://www.vldb.org/conf/2006/p139-xiao.pdf>

# Getting Ready for the Next Privacy and Security Challenges

Reinhard Posch

CIO, Federal Government Austria  
reinhard.posch@cio.gv.at

Cloud, Bring your own Device, Big Data, what have you . . . unless people comply with these Buzzwords they feel to be old-fashioned. Indeed these are often synonyms for big money – but can we understand at all what security and privacy means in this context.

Thanks to Edward Snowden basically everyone talks about privacy. However, unfortunately the impact of the “Snowden effect” on security and privacy might be equally sustainable as the oil crisis was on the global climate change.

Even if this sounds pessimistic the keynote will try to paint a view about what it needs to advance privacy and security at this very point in time where mobile devices, Cloud and collaboration is changing the IT-world dramatically both in dimension and in concept. It is about Europe to take the situation and advance and to sell its leadership in these areas. “eIDaS” the new identity and signature regulation, the new data protection regulation and the NIS directive might be helpful legal instruments helping for European ICT to grow from 28 Member States to a 500 Mio society. Large scale projects arching from examples like STORK to implementation and procurement like Cloud for Europe have a fair chance to be the cornerstones of this development.

Europe has for a long time made profit from its excellence in cryptography and security in academia. Algorithms, concepts and protocols still need to bridge the gap to practical use. While full holomorphic encryption is far from being practical and needing big efforts in research, there are other advances that might be of great help. Privacy preserving authentication and proxy reencryption are just examples helping to close some gaps today in real life.

Given a holistic view of this domain it needs more than just a few algorithmic advances. Pushing up dimension and complexity will not work unless we replace trust by provable trustworthiness and complement this with enabling infrastructures. One such enabling infrastructure will be jurisdiction-aware communication. We must head versus infrastructures that are not limiting communication but identifying jurisdictions data have passed. Then applications and users will be empowered to decide in what environments and jurisdictions they will allow data to flow into and to be received from.

Taking advantage from the momentum NSA and Snowden provide, we need to create environments and infrastructures that allow sustainability and there is ample of challenges ahead. Privacy preserving sharing and collaboration of is one of these big next challenges already emerging.

# Table of Contents

Integrity Assurance for Outsourced Databases without DBMS Modification . . . . .	1
<i>Wei Wei and Ting Yu</i>	
Specification and Deployment of Integrated Security Policies for Outsourced Data . . . . .	17
<i>Anis Bkakra, Frédéric Cuppens, Nora Cuppens-Bouahia, and David Gross-Amblard</i>	
Optimizing Integrity Checks for Join Queries in the Cloud . . . . .	33
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati</i>	
Privacy-Enhancing Proxy Signatures from Non-interactive Anonymous Credentials . . . . .	49
<i>David Derler, Christian Hanser, and Daniel Slamanig</i>	
Privacy-Preserving Multiple Keyword Search on Outsourced Data in the Clouds . . . . .	66
<i>Tarik Moataz, Benjamin Justus, Indrakshi Ray, Nora Cuppens-Bouahia, Frédéric Cuppens, and Indrajit Ray</i>	
Secure and Privacy-Preserving Querying of Personal Health Records in the Cloud . . . . .	82
<i>Samira Barouti, Feras Aljumah, Dima Alhadidi, and Mourad Debbabi</i>	
Data Leakage Quantification . . . . .	98
<i>Sokratis Vavilis, Milan Petković, and Nicola Zannone</i>	
Toward Software Diversity in Heterogeneous Networked Systems . . . . .	114
<i>Chu Huang, Sencun Zhu, and Robert Erbacher</i>	
FSquaDRA: Fast Detection of Repackaged Applications . . . . .	130
<i>Yury Zhauniarovich, Olga Gadyatskaya, Bruno Crispo, Francesco La Spina, and Ermanno Moser</i>	
‘Who, When, and Where?’ Location Proof Assertion for Mobile Devices . . . . .	146
<i>Rasib Khan, Shams Zawoad, Md Munirul Haque, and Ragib Hasan</i>	

Design Patterns for Multiple Stakeholders in Social Computing . . . . .	163
<i>Pooya Mehregan and Philip W.L. Fong</i>	
Collaboratively Solving the Traveling Salesman Problem with Limited Disclosure . . . . .	179
<i>Yuan Hong, Jaideep Vaidya, Haibing Lu, and Lingyu Wang</i>	
ELITE: zEro Links Identity management systEm . . . . .	195
<i>Tarik Moataz, Nora Cuppens-Bouahia, Frédéric Cuppens, Indrajit Ray, and Indrakshi Ray</i>	
Dynamic Workflow Adjustment with Security Constraints . . . . .	211
<i>Haibing Lu, Yuan Hong, Yanjiang Yang, Yi Fang, and Lian Duan</i>	
Consistent Query Plan Generation in Secure Cooperative Data Access . . . . .	227
<i>Meixing Le, Krishna Kant, and Sushil Jajodia</i>	
Hunting the Unknown: White-Box Database Leakage Detection . . . . .	243
<i>Elisa Costante, Jerry den Hartog, Milan Petković, Sandro Etalle, and Mykola Pechenizkiy</i>	
Incremental Analysis of Evolving Administrative Role Based Access Control Policies . . . . .	260
<i>Silvio Ranise and Anh Truong</i>	
Mining Attribute-Based Access Control Policies from Logs . . . . .	276
<i>Zhongyuan Xu and Scott D. Stoller</i>	
Attribute-Aware Relationship-Based Access Control for Online Social Networks . . . . .	292
<i>Yuan Cheng, Jaehong Park, and Ravi Sandhu</i>	
Randomly Partitioned Encryption for Cloud Databases . . . . .	307
<i>Tahmineh Sanamrad, Lucas Braun, Donald Kossmann, and Ramarathnam Venkatesan</i>	
Towards Secure Cloud Database with Fine-Grained Access Control . . . . .	324
<i>Michael G. Solomon, Vaidy Sunderam, and Li Xiong</i>	
Practical Private Information Retrieval from a Time-Varying, Multi-attribute, and Multiple-Occurrence Database . . . . .	339
<i>Giovanni Di Crescenzo, Debra Cook, Allen McIntosh, and Euthimios Panagos</i>	
LPM: Layered Policy Management for Software-Defined Networks . . . . .	356
<i>Wonkyu Han, Hongxin Hu, and Gail-Joon Ahn</i>	
On Minimizing the Size of Encrypted Databases . . . . .	364
<i>Giovanni Di Crescenzo and David Shallcross</i>	

Efficient and Enhanced Solutions for Content Sharing in DRM Systems .....	373
<i>Michal Davidson, Ehud Gudes, and Tamir Tassa</i>	
A Scalable and Efficient Privacy Preserving Global Itemset Support Approximation Using Bloom Filters .....	382
<i>Vikas G. Ashok and Ravi Mukkamala</i>	
<b>Author Index</b> .....	391