

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Shamik Sural · Haibing Lu (Eds.)

Data and Applications Security and Privacy XXXVI

36th Annual IFIP WG 11.3 Conference, DBSec 2022
Newark, NJ, USA, July 18–20, 2022
Proceedings

Editors

Shamik Sural
Department of Computer Science
and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal, India

Haibing Lu
Department of Information Systems
and Analytics
Santa Clara University
Santa Clara, CA, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-10683-5

ISBN 978-3-031-10684-2 (eBook)

<https://doi.org/10.1007/978-3-031-10684-2>

© IFIP International Federation for Information Processing 2022

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.

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.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers selected for presentation at the 36th Annual IFIP WG11.3 Conference on Data and Applications Security and Privacy (DBSec 2022), held during July 18–20, 2022, in Newark, NJ, USA.

In response to the call for papers of this edition, 33 submissions were received, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising 45 members, performed an excellent job, with the help of additional reviewers, of reviewing all submissions through a careful anonymous process (with three or more reviews per submission). The Program Committee's work was carried out electronically, yielding intensive discussions. Of the submitted papers, 12 full papers and six short papers were selected for presentation at the conference.

The success of DBSec 2022 depended on the volunteering effort of many individuals, and there is a long list of people who deserve special thanks. We would like to thank all the members of the Program Committee, and all the external reviewers, for all their hard work in evaluating the papers and for their active participation in the discussion and selection process. We are very grateful to all people who readily assisted and ensured a smooth organization process, in particular Jaideep Vaidya and Yuan Hong for their efforts as DBSec 2022 general co-chairs; Sara Foresti (IFIP WG11.3 chair) for her guidance and support; Hafiz Asif (publicity chair) for helping with publicity; and Lan Yao for helping with other arrangements for the conference. EasyChair made the conference review and proceedings process run very smoothly.

Last but certainly not least, thanks to all the authors who submitted papers and all the conference attendees. We hope you find the proceedings of DBSec 2022 interesting, stimulating, and inspiring for your future research.

June 2022

Shamik Sural
Haibing Lu

Organization

Program Committee

Vijay Atluri	Rutgers University, USA
Yang Cao	Kyoto University, Japan
Frédéric Cuppens	Polytechnique Montréal, Canada
Nora Cuppens-Boulahia	Polytechnique Montréal, Canada
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Giovanni Di Crescenzo	Peraton Labs, USA
Csilla Farkas	University of South Carolina, USA
Barbara Fila	INSA Rennes, IRISA, France
Sara Foresti	Università degli Studi di Milano, Italy
Steven Furnell	University of Nottingham, UK
Kambiz Ghazinour	Kent State University, USA
Ehud Gudes	Ben-Gurion University, Israel
Maanak Gupta	Tennessee Tech University, USA
Yuan Hong	University of Connecticut, USA
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Ram Krishnan	University of Texas at San Antonio, USA
Costas Lambrinoudakis	University of Piraeus, Greece
Adam J. Lee	University of Pittsburgh, USA
Xiang Li	Santa Clara University, USA
Yingjiu Li	University of Oregon, USA
Giovanni Livraga	University of Milan, Italy
Javier Lopez	Universidad de Málaga, Spain
Haibing Lu (Chair)	Santa Clara University, USA
Maryam Majedi	University of Toronto, Canada
Brad Malin	Vanderbilt University, USA
Sjouke Mauw	University of Luxembourg, Luxembourg
Meisam Mohammady	CSIRO, Australia
Samrat Mondal	Indian Institute of Technology Patna, India
Charles Morisset	Newcastle University, UK
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	Università di Bergamo, Italy
Günther Pernul	Universität Regensburg, Germany
Silvio Ranise	University of Trento and Fondazione Bruno Kessler, Italy
Indrajit Ray	Colorado State University, USA

Indrakshi Ray	Colorado State University, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Andreas Schaad	Wibu-Systems, Germany
Anoop Singhal	NIST, USA
Scott Stoller	Stony Brook University, USA
Shamik Sural (Chair)	IIT Kharagpur, India
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	University of Newcastle, Australia
Lingyu Wang	Concordia University, Canada
Edgar Weippl	University of Vienna, Austria
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Contents

Data Privacy

Assessing Differentially Private Variational Autoencoders Under Membership Inference	3
<i>Daniel Bernau, Jonas Robl, and Florian Kerschbaum</i>	
Utility and Privacy Assessment of Synthetic Microbiome Data	15
<i>Markus Hittmeir, Rudolf Mayer, and Andreas Ekelhart</i>	
Combining Defences Against Data-Poisoning Based Backdoor Attacks on Neural Networks	28
<i>Andrea Milakovic and Rudolf Mayer</i>	
MCoM: A Semi-Supervised Method for Imbalanced Tabular Security Data	48
<i>Xiaodi Li, Latifur Khan, Mahmoud Zamani, Shamila Wickramasuriya, Kevin W. Hamlen, and Bhavani Thuraisingham</i>	
Mitigating Privacy Vulnerability Caused by Map Asymmetry	68
<i>Ryota Hiraishi, Masatoshi Yoshikawa, Shun Takagi, Yang Cao, Sumio Fujita, and Hidehito Gomi</i>	

Distributed Systems

Liberate Your Servers: A Decentralized Content Compliance Validation Protocol	89
<i>Bowen Liu and Jianying Zhou</i>	
Knowledge Mining in Cybersecurity: From Attack to Defense	110
<i>Khandakar Ashrafi Akbar, Sadaf Md Halim, Yibo Hu, Anoop Singhal, Latifur Khan, and Bhavani Thuraisingham</i>	
Attack-Resilient Blockchain-Based Decentralized Timed Data Release	123
<i>Jingzhe Wang and Balaji Palanisamy</i>	

IoT Security

Local Intrinsic Dimensionality of IoT Networks for Unsupervised Intrusion Detection	143
<i>Matt Gorbett, Hossein Shirazi, and Indrakshi Ray</i>	

On the Data Privacy, Security, and Risk Postures of IoT Mobile Companion Apps	162
<i>Shradha Neupane, Faiza Tazi, Upakar Paudel, Freddy Veloz Baez, Merzia Adamjee, Lorenzo De Carli, Sanchari Das, and Indrakshi Ray</i>	
Verification and Validation Methods for a Trust-by-Design Framework for the IoT	183
<i>Davide Ferraris, Carmen Fernandez-Gago, and Javier Lopez</i>	
Privacy-Preserving Access and Computation	
Robust and Provably Secure Attribute-Based Encryption Supporting Access Revocation and Outsourced Decryption	197
<i>Anis Bkakria</i>	
Libertas: Backward Private Dynamic Searchable Symmetric Encryption Supporting Wildcards	215
<i>Jeroen Weener, Florian Hahn, and Andreas Peter</i>	
End-to-End Protection of IoT Communications Through Cryptographic Enforcement of Access Control Policies	236
<i>Stefano Berlato, Umberto Morelli, Roberto Carbone, and Silvio Ranise</i>	
Quantum Security	
Integrating and Evaluating Quantum-safe TLS in Database Applications	259
<i>Anselme Tueno, David Boehm, and Shin Ho Choe</i>	
Feel the Quantum Functioning: Instantiating Generic Multi-Input Functional Encryption from Learning with Errors	279
<i>Alexandros Bakas, Antonis Michalas, Eugene Frimpong, and Reyhaneh Rabaninejad</i>	
Security Operations and Policies	
ReLOG: A Unified Framework for Relationship-Based Access Control over Graph Databases	303
<i>Stanley Clark, Nikolay Yakovets, George Fletcher, and Nicola Zannone</i>	
Security Operations Center Roles and Skills: A Comparison of Theory and Practice	316
<i>Andreas Reisser, Manfred Vielberth, Sofia Fohringer, and Günther Pernul</i>	
Author Index	329