



**HAL**  
open science

## Data and Applications Security and Privacy XXXV

Ken Barker, Kambiz Ghazinour

► **To cite this version:**

Ken Barker, Kambiz Ghazinour. Data and Applications Security and Privacy XXXV. Springer International Publishing, LNCS-12840, 2021, Lecture Notes in Computer Science, 978-3-030-81241-6. 10.1007/978-3-030-81242-3 . hal-03677022

**HAL Id: hal-03677022**

**<https://inria.hal.science/hal-03677022v1>**

Submitted on 24 May 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

## 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*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

More information about this subseries at <http://www.springer.com/series/7409>

Ken Barker · Kambiz Ghazinour (Eds.)

# Data and Applications Security and Privacy XXXV

35th Annual IFIP WG 11.3 Conference, DBSec 2021  
Calgary, Canada, July 19–20, 2021  
Proceedings

*Editors*

Ken Barker  
University of Calgary  
Calgary, AB, Canada

Kambiz Ghazinour   
State University of New York at Canton  
Canton, NY, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-81241-6

ISBN 978-3-030-81242-3 (eBook)

<https://doi.org/10.1007/978-3-030-81242-3>

LNCS Sublibrary: SL3 – Information Systems and Applications, incl. Internet/Web, and HCI

© IFIP International Federation for Information Processing 2021

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 35th Annual IFIP WG-11.3 Conference on Data and Applications Security and Privacy (DBSec 2021) that was supposed to take place during July 19–20, 2021, in Calgary, Canada. While the conference was held on the dates as scheduled, due to the COVID-19 situation it was held virtually, but we do look forward to gathering together in 2022 for the next DBSec!

In response to the call for papers for this edition, 45 submissions were received, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising over 40 members, performed an excellent job, with the help of additional reviewers, of reviewing submissions through a careful anonymous process (three or more reviews per submission). The Program Committee's work was carried out electronically, yielding intensive discussions. Of the submitted papers, 15 full papers and 8 short papers were selected for presentation at the conference.

The success of DBSec 2021 depended on the voluntary 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 the people who readily assisted and ensured a smooth organization process, in particular Sara Foresti (IFIP WG11.3 Chair) for her guidance and support, Khosro Salmani as Publicity Chair, and Leanne Wu 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 2021 interesting, stimulating, and inspiring for your future research.

July 2021

Ken Barker  
Kambiz Ghazinour

# Organization

## Program and General Chair

Ken Barker University of Calgary, Canada

## IFIP WG-11.3 Chair

Sara Foresti Università degli Studi di Milano, Italy

## Publicity Chair

Khosro Salmani Mount Royal University, Canada

## Publication Chair

Kambiz Ghazinour State University of New York at Canton,  
USA

## Local Arrangement Chair

Leanne Wu University of Calgary, Canada

## Program Committee

Adam J. Lee	University of Pittsburgh, USA
Andreas Schaad	WIBU-Systems, Germany
Anoop Singhal	NIST, USA
Ayesha Afzal	Air University, USA
Brad Malin	Vanderbilt University, USA
Catherine Meadows	NRL, USA
Charles Morisset	Newcastle University, UK
Costas Lambrinoudakis	University of Piraeus, Greece
Csilla Farkas	University of South Carolina, USA
Edgar Weippl	University of Vienna, Austria
Ehud Gudes	Ben-Gurion University, Israel
Fabio Martinelli	IIT-CNR, Italy
Frédéric Cuppens	Polytechnique Montréal, Canada
Giovanni Di Crescenzo	Perspecta Labs, USA
Giovanni Livraga	University of Milan, Italy

Günther Pernul	Universität Regensburg, Germany
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Jaideep Vaidya	Rutgers University, USA
Javier Lopez	University of Malaga, Spain
Kambiz Ghazinour	State University of New York at Canton, USA
Kui Ren	State University of New York at Buffalo, USA
Lingyu Wang	Concordia University, Canada
Maryam Majedi	University of Toronto, USA
Martin Olivier	University of Pretoria, South Africa
Nicola Zannone	Eindhoven University of Technology, the Netherlands
Nora Cuppens-Boulahia	Polytechnique Montréal, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Sara Foresti	Università degli Studi di Milano, Italy
Scott Stoller	Stony Brook University, USA
Shamik Sural	IIT, Kharagpur, India
Silvio Ranise	FBK-Irst and University of Trento, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Sokratis Katsikas	Open University of Cyprus, Cyprus
Stefano Paraboschi	Università di Bergamo, Italy
Steven Furnell	University of Nottingham, UK
Vijay Atluri	Rutgers University, USA
Vijay Varadharajan	The University of Newcastle, Australia
Wendy Hui Wang	Stevens Institute of Technology, USA
Yingjiu Li	University of Oregon, USA
Yuan Hong	Illinois Institute of Technology, USA

## **Additional Reviewers**

Artsiom Yautsiukhin  
Bingyu Liu  
Giacomo Iadarola  
Han Wang  
Hossein Shirazi  
Stefano Berlato  
Tahir Ahmad  
Xihui Chen  
Yunior Ramírez-Cruz



# Contents

## Differential Privacy

- DPNeT: Differentially Private Network Traffic Synthesis with Generative Adversarial Networks ..... 3  
*Liyue Fan and Akarsh Pokkunuru*
- Comparing Local and Central Differential Privacy Using Membership Inference Attacks ..... 22  
*Daniel Bernau, Jonas Robl, Philip W. Grassal, Steffen Schneider, and Florian Kerschbaum*
- Preventing Manipulation Attack in Local Differential Privacy Using Verifiable Randomization Mechanism ..... 43  
*Fumiyuki Kato, Yang Cao, and Masatoshi Yoshikawa*

## Cryptology I

- Simple Storage-Saving Structure for Volume-Hiding Encrypted Multi-maps: (A Slot in Need is a Slot Indeed) ..... 63  
*Jiafan Wang and Sherman S. M. Chow*
- Nowhere to Leak: A Multi-client Forward and Backward Private Symmetric Searchable Encryption Scheme ..... 84  
*Alexandros Bakas and Antonis Michalas*
- Distributed Query Evaluation over Encrypted Data ..... 96  
*Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati*

## Cryptology II

- Multi-party Private Set Operations with an External Decider ..... 117  
*Sara Ramezani, Tommi Meskanen, and Valteri Niemi*
- Encrypted-Input Obfuscation of Image Classifiers ..... 136  
*Giovanni Di Crescenzo, Lisa Bahler, Brian A. Coan, Kurt Rohloff, David B. Cousins, and Yuriy Polyakov*
- Preserving Privacy of Co-occurring Keywords over Encrypted Data ..... 157  
*D. V. N. Siva Kumar and P. Santhi Thilagam*

**Machine Learning**

Access Control Policy Generation from User Stories Using Machine Learning ..... 171  
*John Heaps, Ram Krishnan, Yufei Huang, Jianwei Niu, and Ravi Sandhu*

PERUN: Confidential Multi-stakeholder Machine Learning Framework with Hardware Acceleration Support ..... 189  
*Wojciech Ozga, Do Le Quoc, and Christof Fetzer*

PDF Malware Detection Using Visualization and Machine Learning ..... 209  
*Ching-Yuan Liu, Min-Yi Chiu, Qi-Xian Huang, and Hung-Min Sun*

Deep Learning for Detecting Network Attacks: An End-to-End Approach ..... 221  
*Qingtian Zou, Anoop Singhal, Xiaoyan Sun, and Peng Liu*

**Potpourri I**

Not a Free Lunch, But a Cheap One: On Classifiers Performance on Anonymized Datasets ..... 237  
*Mina Alishahi and Nicola Zannone*

A Rewarding Framework for Crowdsourcing to Increase Privacy Awareness ... 259  
*Ioannis Chrysakis, Giorgos Flouris, Maria Makridaki, Theodore Patkos, Yannis Roussakis, Georgios Samaritakis, Nikoleta Tsampanaki, Elias Tzortzakakis, Elisjana Ymeralli, Tom Seymoens, Anastasia Dimou, and Ruben Verborgh*

DUCE: Distributed Usage Control Enforcement for Private Data Sharing in Internet of Things ..... 278  
*Na Shi, Bo Tang, Ravi Sandhu, and Qi Li*

**Potpourri II**

A Digital Twin-Based Cyber Range for SOC Analysts ..... 293  
*Manfred Vielberth, Magdalena Glas, Marietheres Dietz, Stylianos Karagiannis, Emmanouil Magkos, and Günther Pernul*

The *tkl*-Score for Data-Sharing Misuseability ..... 312  
*Kalvin Eng and Eleni Stroulia*

Automated Risk Assessment and What-if Analysis of OpenID Connect and OAuth 2.0 Deployments ..... 325  
*Salimeh Dashti, Amir Sharif, Roberto Carbone, and Silvio Ranise*

Divide-and-Learn: A Random Indexing Approach to Attribute Inference  
Attacks in Online Social Networks ..... 338  
*Sanaz Eidizadehakhchelo, Bizhan Alipour Pijani, Abdessamad Imine,  
and Michaël Rusinowitch*

**Access Control**

Verifiable Hierarchical Key Assignment Schemes ..... 357  
*Anna Lisa Ferrara, Federica Paci, and Chiara Ricciardi*

An ABAC Model with Trust and Gossiping (ABAC–TG) for Online Social  
Networks ..... 377  
*Adi Swissa and Ehud Gudes*

On Feasibility of Attribute-Aware Relationship-Based Access Control  
Policy Mining ..... 393  
*Shuvra Chakraborty and Ravi Sandhu*

**Author Index** ..... 407