



HAL
open science

Data and Applications Security and Privacy XXXIV

Anoop Singhal, Jaideep Vaidya

► **To cite this version:**

Anoop Singhal, Jaideep Vaidya. Data and Applications Security and Privacy XXXIV. Springer International Publishing, LNCS-12122, 2020, Lecture Notes in Computer Science, 978-3-030-49668-5. 10.1007/978-3-030-49669-2 . hal-03243621

HAL Id: hal-03243621

<https://inria.hal.science/hal-03243621v1>

Submitted on 31 May 2021

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 series at <http://www.springer.com/series/7409>


Anoop Singhal · Jaideep Vaidya (Eds.)

Data and Applications Security and Privacy XXXIV

34th Annual IFIP WG 11.3 Conference, DBSec 2020
Regensburg, Germany, June 25–26, 2020
Proceedings

Editors

Anoop Singhal
National Institute of Standards
and Technology
Gaithersburg, MD, USA

Jaideep Vaidya 
Rutgers University
Newark, NJ, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-49668-5 ISBN 978-3-030-49669-2 (eBook)
<https://doi.org/10.1007/978-3-030-49669-2>

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

© IFIP International Federation for Information Processing 2020

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, express 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 34th Annual IFIP WG11.3 Conference on Data and Applications Security and Privacy (DBSec 2020), that was supposed to be during June 25–26, 2020, in Regensburg. While the conference was held on the dates as scheduled, due to the COVID-19 situation it was held virtually (for the first time in the history of DBSec), instead of physically in Regensburg.

In response to the call for papers of this edition, 41 submissions were received, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising 40 members, performed an excellent job, with the help of additional reviewers, of reviewing all 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, 14 full papers and 8 short papers were selected for presentation at the conference.

The success of DBSec 2020 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 Günther Pernul for his efforts as DBSec 2020 general chair; Sara Foresti (IFIP WG11.3 chair) for her guidance and support; Yuan Hong and Benedikt Putz (publicity chairs) for helping with publicity; and Petra Sauer 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 2020 interesting, stimulating, and inspiring for your future research.

April 2020

Anoop Singhal
Jaideep Vaidya

Organization

Program Committee

Ayesha Afzal	Air University, USA
Vijay Atluri	Rutgers University, USA
Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	IMT Atlantique, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Giovanni Di Crescenzo	Perspecta Labs, USA
Csilla Farkas	USC, USA
Barbara Fila	INSA Rennes, IRISA, France
Sara Foresti	Università degli Studi di Milano, Italy
Steven Furnell	Plymouth University, UK
Ehud Gudes	Ben-Gurion University, Israel
Yuan Hong	Illinois Institute of Technology, USA
Sokratis Katsikas	Open University of Cyprus, Cyprus
Costas Lambrinoudakis	University of Piraeus, Greece
Adam J. Lee	University of Pittsburgh, USA
Yingjiu Li	University of Oregon, USA
Giovanni Livraga	University of Milan, Italy
Javier Lopez	UMA, Spain
Brad Malin	Vanderbilt University, USA
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	NRL, USA
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	FBK-Irst, Italy
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Kui Ren	State University of New York at Buffalo, 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	IIT Kharagpur, India
Jaideep Vaidya	Rutgers University, Australia
Vijay Varadharajan	The University of Newcastle, Australia

Lingyu Wang	Concordia University, Canada
Wendy Hui Wang	Stevens Institute of Technology, USA
Edgar Weippl	University of Vienna, Austria
Attila A. Yavuz	University of South Florida, USA
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Additional Reviewers

Alcaraz, Cristina	Mohamady, Meisam
Berlato, Stefano	Mykoniati, Maria
Binder, Dominik	Nieto, Ana
Bursuc, Sergiu	Roman, Rodrigo
Chen, Xihui	Sascha, Kern
Clark, Stanley	Schlette, Daniel
Derbeko, Philip	Sciarretta, Giada
Georgiopoulou, Zafeiroula	Shafiq, Basit
Groll, Sebastian	Thang, Hoang
Haefner, Kyle	Voloch, Nadav
Liu, Bingyu	Wan, Zhiyu
Liu, Yongtai	Wang, Han
Lyvas, Christos	Yan, Chao

Contents

Network and Cyber-Physical Systems Security

Modeling and Mitigating Security Threats in Network Functions Virtualization (NFV)	3
<i>Nawaf Alhebaishi, Lingyu Wang, and Sushil Jajodia</i>	
Managing Secure Inter-slice Communication in 5G Network Slice Chains . . .	24
<i>Luis Suárez, David Espes, Frédéric Cuppens, Cao-Thanh Phan, Philippe Bertin, and Philippe Le Parc</i>	
Proactively Extracting IoT Device Capabilities: An Application to Smart Homes	42
<i>Andy Dolan, Indrakshi Ray, and Suryadipta Majumdar</i>	
Security Enumerations for Cyber-Physical Systems	64
<i>Daniel Schlette, Florian Menges, Thomas Baumer, and Günther Pernul</i>	

Information Flow and Access Control

Inference-Proof Monotonic Query Evaluation and View Generation Reconsidered	79
<i>Joachim Biskup</i>	
Network Functions Virtualization Access Control as a Service	100
<i>Manel Smine, David Espes, Nora Cuppens-Boulahia, and Frédéric Cuppens</i>	
Effective Access Control in Shared-Operator Multi-tenant Data Stream Management Systems	118
<i>Marian Zaki, Adam J. Lee, and Panos K. Chrysanthis</i>	
Information Flow Security Certification for SPARK Programs	137
<i>Sandip Ghosal and R. K. Shyamasundar</i>	

Privacy-Preserving Computation

Provably Privacy-Preserving Distributed Data Aggregation in Smart Grids . . .	153
<i>Marius Stübs, Tobias Mueller, Kai Bavendiek, Manuel Loesch, Sibylle Schupp, and Hannes Federrath</i>	
Non-interactive Private Decision Tree Evaluation	174
<i>Anselme Tueno, Yordan Boev, and Florian Kerschbaum</i>	

Privacy-Preserving Anomaly Detection Using Synthetic Data	195
<i>Rudolf Mayer, Markus Hittmeir, and Andreas Ekelhart</i>	
Local Differentially Private Matrix Factorization with MoG for Recommendations.	208
<i>Jeyamohan Neera, Xiaomin Chen, Nauman Aslam, and Zhan Shu</i>	
Visualization and Analytics for Security	
Designing a Decision-Support Visualization for Live Digital Forensic Investigations.	223
<i>Fabian Böhm, Ludwig Englbrecht, and Günther Pernul</i>	
Predictive Analytics to Prevent Voice over IP International Revenue Sharing Fraud	241
<i>Yoram J. Meijaard, Bram C. M. Cappers, Josh G. M. Mengerink, and Nicola Zannone</i>	
PUA Detection Based on Bundle Installer Characteristics.	261
<i>Amir Lukach, Ehud Gudes, and Asaf Shabtai</i>	
ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool.	274
<i>Andreas Schaad and Dominik Binder</i>	
Spatial Systems and Crowdsourcing Security	
Enhancing the Performance of Spatial Queries on Encrypted Data Through Graph Embedding.	289
<i>Sina Shaham, Gabriel Ghinita, and Cyrus Shahabi</i>	
Crowdsourcing Under Data Poisoning Attacks: A Comparative Study	310
<i>Farnaz Tahmasebian, Li Xiong, Mani Sotoodeh, and Vaidy Sunderam</i>	
Self-enhancing GPS-Based Authentication Using Corresponding Address.	333
<i>Tran Phuong Thao, Mhd Irvan, Ryosuke Kobayashi, Rie Shigetomi Yamaguchi, and Toshiyuki Nakata</i>	
Secure Outsourcing and Privacy	
GOOSE: A Secure Framework for Graph Outsourcing and SPARQL Evaluation	347
<i>Radu Ciucanu and Pascal Lafourcade</i>	
SGX-IR: Secure Information Retrieval with Trusted Processors.	367
<i>Fahad Shaon and Murat Kantarcioglu</i>	

Readability of Privacy Policies	388
<i>Barbara Krumay and Jennifer Klar</i>	
Author Index	401