# Data and Applications Security and Privacy XXXIV

Anoop Singhal, Jaideep Vaidya

# Lecture Notes in Computer Science 12122

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

Springer

*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

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

# Contents

## Network and Cyber-Physical Systems Security

Modeling and Mitigating Security Threats in Network Functions Virtualization (NFV) . . . 3
*Nawaf Alhebaishi, Lingyu Wang, and Sushil Jajodia*

Managing Secure Inter-slice Communication in 5G Network Slice Chains . . . 24
*Luis Suárez, David Espes, Frédéric Cuppens, Cao-Thanh Phan, Philippe Bertin, and Philippe Le Parc*

Proactively Extracting IoT Device Capabilities: An Application to Smart Homes . . . 42
*Andy Dolan, Indrakshi Ray, and Suryadipta Majumdar*

Security Enumerations for Cyber-Physical Systems . . . 64
*Daniel Schlette, Florian Menges, Thomas Baumer, and Günther Pernul*

## Information Flow and Access Control

Inference-Proof Monotonic Query Evaluation and View Generation Reconsidered . . . 79
*Joachim Biskup*

Network Functions Virtualization Access Control as a Service . . . 100
*Manel Smine, David Espes, Nora Cuppens-Boulahia, and Frédéric Cuppens*

Effective Access Control in Shared-Operator Multi-tenant Data Stream Management Systems . . . 118
*Marian Zaki, Adam J. Lee, and Panos K. Chrysanthis*

Information Flow Security Certification for SPARK Programs . . . 137
*Sandip Ghosal and R. K. Shyamasundar*

## Privacy-Preserving Computation

Provably Privacy-Preserving Distributed Data Aggregation in Smart Grids . . . 153
*Marius Stübs, Tobias Mueller, Kai Bavendiek, Manuel Loesch, Sibylle Schupp, and Hannes Federrath*

Non-interactive Private Decision Tree Evaluation . . . 174
*Anselme Tueno, Yordan Boev, and Florian Kerschbaum*

Privacy-Preserving Anomaly Detection Using Synthetic Data . . . . . . . . . . . . 195
*Rudolf Mayer, Markus Hittmeir, and Andreas Ekelhart*

Local Differentially Private Matrix Factorization with MoG for Recommendations. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 208
*Jeyamohan Neera, Xiaomin Chen, Nauman Aslam, and Zhan Shu*

**Visualization and Analytics for Security**

Designing a Decision-Support Visualization for Live Digital Forensic Investigations. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 223
*Fabian Böhm, Ludwig Englbrecht, and Günther Pernul*

Predictive Analytics to Prevent Voice over IP International Revenue Sharing Fraud . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 241
*Yoram J. Meijaard, Bram C. M. Cappers, Josh G. M. Mengerink, and Nicola Zannone*

PUA Detection Based on Bundle Installer Characteristics. . . . . . . . . . . . . . . . 261
*Amir Lukach, Ehud Gudes, and Asaf Shabtai*

ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 274
*Andreas Schaad and Dominik Binder*

**Spatial Systems and Crowdsourcing Security**

Enhancing the Performance of Spatial Queries on Encrypted Data Through Graph Embedding. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 289
*Sina Shaham, Gabriel Ghinita, and Cyrus Shahabi*

Crowdsourcing Under Data Poisoning Attacks: A Comparative Study . . . . . . 310
*Farnaz Tahmasebian, Li Xiong, Mani Sotoodeh, and Vaidy Sunderam*

Self-enhancing GPS-Based Authentication Using Corresponding Address. . . . 333
*Tran Phuong Thao, Mhd Irvan, Ryosuke Kobayashi, Rie Shigetomi Yamaguchi, and Toshiyuki Nakata*

**Secure Outsourcing and Privacy**

GOOSE: A Secure Framework for Graph Outsourcing and SPARQL Evaluation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 347
*Radu Ciucanu and Pascal Lafourcade*

SGX-IR: Secure Information Retrieval with Trusted Processors. . . . . . . . . . . 367
*Fahad Shaon and Murat Kantarcioglu*

Readability of Privacy Policies . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 388
*Barbara Krumay and Jennifer Klar*

**Author Index** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 401