

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board Members

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology Madras, Chennai, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

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

Simon N. Foley (Ed.)

# Data and Applications Security and Privacy XXXIII

33rd Annual IFIP WG 11.3 Conference, DBSec 2019  
Charleston, SC, USA, July 15–17, 2019  
Proceedings

*Editor*  
Simon N. Foley  
Norwegian University of Science  
and Technology  
Gjøvik, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-22478-3 ISBN 978-3-030-22479-0 (eBook)  
<https://doi.org/10.1007/978-3-030-22479-0>

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

© IFIP International Federation for Information Processing 2019

The chapter “Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping” is Open Access. This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

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 book contains the papers that were selected for presentation and publication at the 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2019) that was held in Charleston, South Carolina, USA, July 15–17, 2019.

The Program Committee accepted 21 papers out of a total of 51 papers that were submitted from 18 different countries. The papers in this book are drawn from a range of topics, including privacy, code security, security threats, security protocols, distributed systems, and mobile and Web security. The 43-member Program Committee, assisted by a further 43 external reviewers, reviewed and discussed the papers online over a period of over six weeks and with each paper receiving at least three reviews.

DBSec 2019 would not have been possible without the contributions of the many volunteers who freely gave their time and expertise. Our thanks go to the members of the Program Committee and the external reviewers for their work in evaluating the papers. Grateful thanks are due to all the people who gave their assistance and ensured a smooth organization, in particular Csilla Farkas and Mark Daniels for their efforts as DBSec 2019 general chairs; Sabrina De Capitani di Vimercati (IFIP WG11.3 Chair) for her guidance and support, and Emad Alsuwat for managing the conference website. A special thanks goes to the invited speakers for their keynote presentations. Finally, we would like to express our thanks to the authors who submitted papers to DBSec. They, more than anyone else, are what makes this conference possible.

July 2019

Simon Foley

# Organization

## IFIP WG 11.3 Chair

Sabrina De Capitani di  
Vimercati                      Università degli Studi di Milano, Italy

## General Chairs

Csilla Farkas                      University of South Carolina, USA  
Mark Daniels                      Medical University of South Carolina, USA

## Program Chair

Simon Foley                      Norwegian University of Science and Technology,  
Norway

## Program Committee

Vijay Atluri                      Rutgers University, USA  
Frédéric Cuppens                      IMT Atlantique, France  
Nora Cuppens-Boulahia                      IMT Atlantique, France  
Sabrina De Capitani di  
Vimercati                      University of Milan, Italy  
Giovanni Di Crescenzo                      Perspecta Labs, USA  
Wenliang Du                      Syracuse University, USA  
Barbara Fila                      INSA Rennes, IRISA, France  
Simon Foley                      Norwegian University of Science and Technology,  
Norway  
Sara Foresti                      University of Milan, Italy  
Joaquin Garcia-Alfaro                      Telecom SudParis, France  
Stefanos Gritzalis                      University of the Aegean, Greece  
Ehud Gudes                      Ben-Gurion University, Israel  
Yuan Hong                      Illinois Institute of Technology, USA  
Sokratis Katsikas                      Norwegian University of Science and Technology,  
Norway  
Florian Kerschbaum                      University of Waterloo, Canada  
Adam J. Lee                      University of Pittsburgh, USA  
Yingjiu Li                      Singapore Management University, Singapore  
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  | University of Bergamo, Italy                        |
| Günther Pernul      | Universität Regensburg, Germany                     |
| Andreas Peter       | University of Twente, The Netherlands               |
| Silvio Ranise       | FBK-Irst, Italy                                     |
| Indrajit Ray        | Colorado State University, USA                      |
| Kui Ren             | State University of New York at Buffalo, USA        |
| Pierangela Samarati | University of Milan, Italy                          |
| Andreas Schaad      | WIBU-Systems, Germany                               |
| Scott Stoller       | Stony Brook University, USA                         |
| Tamir Tassa         | The Open University of Israel, Israel               |
| Mahesh Tripunitara  | University of Waterloo, Canada                      |
| Jaideep Vaidya      | Rutgers University, USA                             |
| Vijay Varadharajan  | The University of Newcastle, Australia              |
| Lingyu Wang         | Concordia University, Canada                        |
| Wendy Hui Wang      | Stevens Institute of Technology, USA                |
| Attila A Yavuz      | University of South Florida, USA                    |
| Ting Yu             | Qatar Computing Research Institute, Qatar           |
| Nicola Zannone      | Eindhoven University of Technology, The Netherlands |

## Additional Reviewers

|                         |                          |
|-------------------------|--------------------------|
| Ahlawat, Amit           | Oqaily, Alaa             |
| Akowuah, Francis        | Oqaily, Momen            |
| Alhebaishi, Nawaf       | Ozmen, Muslum Ozgur      |
| Anagnostopoulos, Marios | Puchtra, Alexander       |
| Asadi, Behzad           | Ramírez-Cruz, Yuniór     |
| Behnia, Rouzbeh         | Rizos, Athanasios        |
| Bui, Thang              | Sengupta, Binanda        |
| Ceccato, Mariano        | Seyitoglu, Efe Ulas Akay |
| Cledel, Thomas          | Tian, Yangguang          |
| Dietz, Marietheres      | Tsohou, Aggeliki         |
| Esquivel-Vargas, Herson | Uganbayar, Ganbayar      |
| Fernandez, Gerardo      | van de Kamp, Tim         |
| Gadyatskaya, Olga       | van Deursen, Ton         |
| Hitchens, Michael       | Vielberth, Manfred       |
| Hoang, Thang            | Voloch, Nadav            |
| Kalloniatis, Christos   | Wang, Han                |
| Liu, Bingyu             | Widel, Wojciech          |
| Luo, Meng               | Xie, Shangyu             |
| Mercaldo, Francesco     | Xu, Jiayun               |
| Michailidou, Christina  | Xu, Shengmin             |
| Mohammady, Meisam       | Zhang, Mingwei           |
| Mueller, Johannes       |                          |

# Contents

## Attacks

|  |    |
|--|----|
| Detecting Adversarial Attacks in the Context of Bayesian Networks . . . . .                  | 3  |
| <i>Emad Alsuwat, Hatim Alsuwat, John Rose, Marco Valtorta, and Csilla Farkas</i>             |    |
| AGBuilder: An AI Tool for Automated Attack Graph Building, Analysis, and Refinement. . . . . | 23 |
| <i>Bruhadeshwar Bezawada, Indrajit Ray, and Kushagra Tiwary</i>                              |    |
| On Practical Aspects of PCFG Password Cracking . . . . .                                     | 43 |
| <i>Radek Hranický, Filip Lištiak, Dávid Mikuš, and Ondřej Ryšavý</i>                         |    |
| That’s My DNA: Detecting Malicious Tampering of Synthesized DNA . . . . .                    | 61 |
| <i>Diptendu Mohan Kar and Indrajit Ray</i>   |    |

## Mobile and Web Security

|  |     |
|--|-----|
| Adversarial Sampling Attacks Against Phishing Detection . . . . .                                | 83  |
| <i>Hossein Shirazi, Bruhadeshwar Bezawada, Indrakshi Ray, and Charles Anderson</i>               |     |
| Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping . . . . . | 102 |
| <i>Jacob Leon Kröger and Philip Raschke</i>  |     |
| Droids in Disarray: Detecting <i>Frame Confusion</i> in Hybrid Android Apps. . . . .             | 121 |
| <i>Davide Caputo, Luca Verderame, Simone Aonzo, and Alessio Merlo</i>                            |     |

## Privacy

|  |     |
|--|-----|
| Geo-Graph-Indistinguishability: Protecting Location Privacy for LBS over Road Networks . . . . .                                 | 143 |
| <i>Shun Takagi, Yang Cao, Yasuhito Asano, and Masatoshi Yoshikawa</i>  |     |
| “When and Where Do You Want to Hide?” – Recommendation of Location Privacy Preferences with Local Differential Privacy . . . . . | 164 |
| <i>Maho Asada, Masatoshi Yoshikawa, and Yang Cao</i>   |     |

Analysis of Privacy Policies to Enhance Informed Consent . . . . . 177  
*Raúl Pardo and Daniel Le Métayer*

**Security Protocol Practices**

Lost in TLS? No More! Assisted Deployment of Secure TLS  
Configurations . . . . . 201  
*Salvatore Manfredi, Silvio Ranise, and Giada Sciarretta*

Contributing to Current Challenges in Identity and Access Management  
with Visual Analytics . . . . . 221  
*Alexander Puchta, Fabian Böhm, and Günther Pernul*

Analysis of Multi-path Onion Routing-Based Anonymization Networks . . . . . 240  
*Wladimir De la Cadena, Daniel Kaiser, Asya Mitseva,  
Andriy Panchenko, and Thomas Engel*

**Distributed Systems**

Shoal: Query Optimization and Operator Placement for Access  
Controlled Stream Processing Systems . . . . . 261  
*Cory Thoma, Alexandros Labrinidis, and Adam J. Lee*

A Distributed Ledger Approach to Digital Twin Secure Data Sharing . . . . . 281  
*Marietheres Dietz, Benedikt Putz, and Günther Pernul*

Refresh Instead of Revoke Enhances Safety and Availability:  
A Formal Analysis . . . . . 301  
*Mehrnoosh Shakarami and Ravi Sandhu*

**Source Code Security**

Wrangling in the Power of Code Pointers with ProxyCFI . . . . . 317  
*Misiker Tadesse Aga, Colton Holoday, and Todd Austin*

CASFinder: Detecting Common Attack Surface . . . . . 338  
*Mengyuan Zhang, Yue Xin, Lingyu Wang, Sushil Jajodia,  
and Anoop Singhal*

Algorithm Diversity for Resilient Systems . . . . . 359  
*Scott D. Stoller and Yanhong A. Liu*

**Malware**

Online Malware Detection in Cloud Auto-scaling Systems Using  
Shallow Convolutional Neural Networks ..... 381  
*Mahmoud Abdelsalam, Ram Krishnan, and Ravi Sandhu*

Redirecting Malware’s Target Selection with Decoy Processes ..... 398  
*Sara Sutton, Garret Michilli, and Julian Rrushi*

**Author Index** ..... 419