

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Florian Kerschbaum · Stefano Paraboschi (Eds.)

Data and Applications Security and Privacy XXXII

32nd Annual IFIP WG 11.3 Conference, DBSec 2018
Bergamo, Italy, July 16–18, 2018
Proceedings

Editors

Florian Kerschbaum
University of Waterloo
Waterloo, ON
Canada

Stefano Paraboschi
Università degli Studi di Bergamo
Dalmine
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-95728-9 ISBN 978-3-319-95729-6 (eBook)
<https://doi.org/10.1007/978-3-319-95729-6>

Library of Congress Control Number: 2018947573

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

© IFIP International Federation for Information Processing 2018

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.

Printed on acid-free paper

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 32nd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2018), held in Bergamo, Italy, during July 16–18, 2018.

In response to the call for papers of this edition, 50 submissions were received, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising 36 members, performed an excellent task and with the help of additional reviewers all submissions went through a careful anonymous review process (three or more reviews per submission). The Program Committee's work was carried out electronically, yielding intensive discussions. Of the submitted papers, 16 full papers and five short papers were selected for presentation at the conference.

The success of DBSec 2018 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 gave their assistance and ensured a smooth organization process, in particular Sara Foresti for her efforts as DBSec 2018 general chair; Sabrina De Capitani di Vimercati (IFIP WG11.3 chair) for her guidance and support; and Enrico Bacis and Marco Rosa (publicity chairs) for helping with publicity. A special thanks goes to the keynote speakers, who accepted our invitation to deliver a keynote talk at the conference.

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 2018 interesting, stimulating, and inspiring for your future research.

June 2018

Florian Kerschbaum
Stefano Paraboschi

Organization

Program Committee

Frederik Armknecht	Universität Mannheim, Germany
Vijay Atluri	Rutgers University, USA
Frédéric Cuppens	Telecom Bretagne, France
Nora Cuppens-Boulahia	IMT Atlantique, France
Sabrina De Capitani di Vimercati	University of Milan, Italy
Giovanni Di Crescenzo	Vencore Labs, USA
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
Sushil Jajodia	George Mason University, USA
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Alex Liu	Michigan State University, USA
Peng Liu	The Pennsylvania State University, USA
Giovanni Livraga	University of Milan, Italy
Ashwin Machanavajjhala	Duke University, USA
Brad Malin	Vanderbilt University, USA
Catherine Meadows	NRL, USA
Martin Olivier	University of Pretoria, South Africa
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
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
Lingyu Wang	Concordia University, Canada
Wendy Hui Wang	Stevens Institute of Technology, USA
Attila A. Yavuz	Oregon State University, USA
Ting Yu	Qatar Computing Research Institute, Qatar
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Additional Reviewers

Alhebaishi, Nawaf

Bacis, Enrico

Behnia, Rouzbeh

Bernau, Daniel

Bezawada, Bruhadeshwar

Boehler, Jonas

Borbor, Daniel

Bui, Thang

Bösch, Christoph

Fischer, Andreas

Fuhry, Benny

Kar, Diptendu Mohan

Lei, Xinyu

Majumdar, Suryadipta

Makri, Eleftheria

Oqaily, Alaa

Ozmen, Muslum Ozgur

Rindal, Peter

Rosa, Marco

Siena, Alberto

Thang, Hoang

Tueno, Anselme

Venkatesan, Sridhar

Voloch, Nadav

Wang, Han

Weggenmann, Benjamin

Xie, Shangyu

Zhang, Bo

Contents

Administration

Modeling and Mitigating the Insider Threat of Remote Administrators in Clouds	3
<i>Nawaf Alhebaishi, Lingyu Wang, Sushil Jajodia, and Anoop Singhal</i>	
Blockchain-Based Auditing of Transparent Log Servers	21
<i>Hoang-Long Nguyen, Jean-Philippe Eisenbarth, Claudia-Lavinia Ignat, and Olivier Perrin</i>	
Probabilistic Event Graph to Model Safety and Security for Diagnosis Purposes	38
<i>Edwin Bourget, Frédéric Cuppens, Nora Cuppens-Boulahia, Samuel Dubus, Simon Foley, and Youssef Laarouchi</i>	

Access Control Policies

Enabling the Deployment of ABAC Policies in RBAC Systems	51
<i>Gunjan Batra, Vijayalakshmi Atluri, Jaideep Vaidya, and Shamik Sural</i>	
Policy Languages and Their Suitability for Trust Negotiation	69
<i>Martin Kolar, Carmen Fernandez-Gago, and Javier Lopez</i>	
Role of Apps in Undoing of Privacy Policies on Facebook	85
<i>Vishwas T. Patil, Nivia Jatain, and R. K. Shyamasundar</i>	
Towards Adaptive Access Control.	99
<i>Luciano Argento, Andrea Margheri, Federica Paci, Vladimiro Sassone, and Nicola Zannone</i>	

Privacy-Preserving Access and Computation

Oblivious Dynamic Searchable Encryption on Distributed Cloud Systems . . .	113
<i>Thang Hoang, Attila A. Yavuz, F. Betül Durak, and Jorge Guajardo</i>	
Privacy-Preserving Planarity Testing of Distributed Graphs	131
<i>Guy Barshap and Tamir Tassa</i>	
Image Pixelization with Differential Privacy	148
<i>Liyue Fan</i>	

Integrity and User Interaction

Data Integrity Verification in Column-Oriented NoSQL Databases 165
Grisha Weintraub and Ehud Gudes

A Novel Hybrid Password Authentication Scheme Based on Text
and Image 182
Ian Mackie and Merve Yildirim

“It’s Shocking!”: Analysing the Impact and Reactions to the A3:
Android Apps Behaviour Analyser 198
*Majid Hatamian, Agnieszka Kitkowska, Jana Korunovska,
and Sabrina Kirrane*

Security Analysis and Private Evaluation

FlowConSEAL: Automatic Flow Consistency Analysis of SEAndroid
and SELinux Policies 219
B. S. Radhika, N. V. Narendra Kumar, and R. K. Shyamasundar

On Understanding Permission Usage Contextuality in Android Apps. 232
Md Zakir Hossen and Mohammad Mannan

Private yet Efficient Decision Tree Evaluation 243
Marc Joye and Fariborz Salehi

Fixing Vulnerabilities

Breaking and Fixing the Security Proof of Garbled Bloom Filters 263
Cédric Van Rompay and Melek Önen

USBLOCK: Blocking USB-Based Keypress Injection Attacks 278
*Sebastian Neuner, Artemios G. Voyiatzis, Spiros Fotopoulos,
Collin Mulliner, and Edgar R. Weippl*

Networked Systems

Virtually Isolated Network: A Hybrid Network to Achieve High
Level Security 299
Jia Xu and Jianying Zhou

Fingerprinting Crowd Events in Content Delivery Networks:
A Semi-supervised Methodology. 312
*Amine Boukhtouta, Makan Pourzandi, Richard Brunner,
and Stéphane Dault*

Assessing Attack Impact on Business Processes by Interconnecting
Attack Graphs and Entity Dependency Graphs 330
*Chen Cao, Lun-Pin Yuan, Anoop Singhal, Peng Liu, Xiaoyan Sun,
and Sencun Zhu*

Author Index 349