

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/7410>


Nur Zincir-Heywood · Guillaume Bonfante ·
Mourad Debbabi · Joaquin Garcia-Alfaro (Eds.)

Foundations and Practice of Security


11th International Symposium, FPS 2018
Montreal, QC, Canada, November 13–15, 2018
Revised Selected Papers

Editors

Nur Zincir-Heywood
Dalhousie University
Halifax, NS, Canada

Mourad Debbabi 
Concordia University
Montreal, QC, Canada

Guillaume Bonfante
École des Mines de Nancy
Nancy, France

Joaquin Garcia-Alfaro 
Telecom SudParis
Evry, France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-18418-6 ISBN 978-3-030-18419-3 (eBook)
<https://doi.org/10.1007/978-3-030-18419-3>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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 presented at the 11th International Symposium on Foundations and Practice of Security (FPS 2018), which was held at Gina Cody School of Engineering and Computer Science, Concordia University, Montreal, Quebec, Canada, during November 13–15, 2018. The Symposium received 51 submissions, from countries all over the world. Each paper was reviewed by at least three committee members. The Program Committee selected 16 full papers for presentation. The program was completed with one short paper and one position paper, and three excellent invited talks given by Guang Gong (University of Waterloo), Sanjay Goel (University at Albany, SUNY) and Sébastien Gambs (Université du Québec à Montréal, UQAM). At least three reviews were given for each submitted paper. The decision on acceptance or rejection in the review process was completed after intensive discussions over a period of one week.

Many people contributed to the success of FPS 2018. First, we would like to thank all the authors who submitted their research results. The selection was a challenging task and we sincerely thank all the Program Committee members, as well as the external reviewers, who volunteer to read and discuss the papers. We greatly thank the general chair, Frédéric Cuppens (IMT Atlantique); the organization chair, Amr Youssef (Concordia University, Canada); the local organization chairs, Paria Shirani (Concordia University, Canada) and Jun Yan (Concordia University, Canada); and the publications and publicity chairs, Arash Mohammadi (Concordia University, Canada) and Joaquin Garcia-Alfaro (IMT, Paris-Saclay, France). We also want to express our gratitude to all the attendees and volunteers. Last but, by no means least, we want to thank all the sponsors for making the event possible.

We hope the articles contained in this proceedings volume will be valuable for your professional activities in the area.

February 2019

Nur Zincir-Heywood
Guillaume Bonfante
Mourad Debbabi

Organization

General Chair

Frédéric Cuppens IMT Atlantique, France

Program Co-chairs

Nur Zincir-Heywood Dalhousie University, Canada
Guillaume Bonfante Ecole des Mines de Nancy, France
Mourad Debbabi Concordia University, Canada

Publications and Publicity Chairs

Arash Mohammadi Concordia University, Canada
Joaquin Garcia-Alfaro Télécom SudParis, France

Organization Chair

Amr Youssef Concordia University, Canada

Local Organization Chairs

Paria Shirani Concordia University, Canada
Jun Yan Concordia University, Canada

Program Committee

Esma Aimeur University of Montreal, Canada
Jeremy Clark Concordia University, Canada
Nora Cuppens IMT Atlantique, France
Frédéric Cuppens IMT Atlantique, France
Jean-Luc Danger Télécom Paris-Tech, France
Mourad Debbabi Concordia University, Canada
Josée Desharnais Laval University, Canada
Samuel Dubus NOKIA Bell Labs, France
Joaquin Garcia-Alfaro Télécom SudParis, France
Dieter Gollmann Hamburg University of Technology, Germany
Sushil Jajodia George Mason University, USA
Bruce Kapron University of Victoria, Canada
Raphaël Khoury Université du Québec à Chicoutimi, Canada
Hyoungshick Kim Sungkyunkwan University, Republic of Korea
Igor Kotenko SPIIRAS, Russia

Evangelos Kranakis	Carleton University Computer Science, Canada
Pascal Lafourcade	Université d'Auvergne, France
Luigi Logrippo	Université du Québec en Outaouais, Canada
Suryadipta Majumdar	University at Albany, USA
Fabio Martinelli	National Research Council of Italy (CNR), Italy
Paliath Narendran	University at Albany, USA
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Jun Pang	University of Luxembourg, Luxembourg
Marie-Laure Potet	VERIMAG, France
Silvio Ranise	FBK, Security and Trust Unit, Italy
Indrakshi Ray	Colorado State University, USA
Michaël Rusinowitch	LORIA-Inria Nancy, France
Paria Shirani	Concordia University, Canada
Natalia Stakhonova	University of New Brunswick, Canada
Chamseddine Talhi	École de Technologie Supérieure, Canada
Nadia Tawbi	Université Laval, Canada
Lingyu Wang	Concordia University, Canada
Edgar Weippl	SBA Research, Austria
Lena Wiese	Georg-August Universität Göttingen, Germany
Xun Yi	RMIT University, Australia
Nur Zincir-Heywood	Dalhousie University, Canada
Mohammad Zulkernine	Queen's University, Canada

Steering Committee

Frédéric Cuppens	IMT Atlantique, France
Nora Cuppens-Boulahia	IMT Atlantique, France
Mourad Debbabi	University of Concordia, Canada
Joaquin Garcia-Alfaro	Télécom SudParis, France
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	Université d'Auvergne, France
Jean-Yves Marion	Mines de Nancy, France
Ali Miri	Ryerson University, Canada
Rei Safavi-Naini	Calgary University, Canada
Nadia Tawbi	Université Laval, Canada

Contents

Invited Papers

Securing Internet-of-Things	3
<i>Guang Gong</i>	
Privacy and Ethical Challenges in Big Data	17
<i>Sébastien Gambs</i>	

Mobile Security

Decentralized Dynamic Security Enforcement for Mobile Applications with CliSeAuDroid	29
<i>Tobias Hamann and Heiko Mantel</i>	
Mobile Travel Credentials	46
<i>David Bissessar, Maryam Hezaveh, Fayzah Alshammari, and Carlisle Adams</i>	

Cloud Security and Big Data

Cloud Security Auditing: Major Approaches and Existing Challenges	61
<i>Suryadipta Majumdar, Taous Madi, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	
Secure Joins with MapReduce	78
<i>Xavier Bultel, Radu Ciucanu, Matthieu Giraud, Pascal Lafourcade, and Lihua Ye</i>	
Daedalus: Network Anomaly Detection on IDS Stream Logs	95
<i>Aniss Chohra, Mourad Debbabi, and Paria Shirani</i>	

IoT Security

Configuring Data Flows in the Internet of Things for Security and Privacy Requirements	115
<i>Luigi Logrippo and Abdelouadoud Stambouli</i>	
Validating Requirements of Access Control for Cloud-Edge IoT Solutions (Short Paper)	131
<i>Tahir Ahmad and Silvio Ranise</i>	

Software Security, Malware Analysis, and Vulnerability Detection

Evading Deep Neural Network and Random Forest Classifiers by Generating Adversarial Samples	143
<i>Erick Eduardo Bernal Martinez, Bella Oh, Feng Li, and Xiao Luo</i>	
Protection of Systems Against Fuzzing Attacks.	156
<i>Léopold Ouairy, Hélène Le-Bouder, and Jean-Louis Lanet</i>	
A Comparative Study Across Static and Dynamic Side-Channel Countermeasures	173
<i>Yuri Gil Dantas, Tobias Hamann, and Heiko Mantel</i>	

Cryptography

Card-Based Cryptographic Protocols with the Minimum Number of Cards Using Private Operations	193
<i>Hibiki Ono and Yoshifumi Manabe</i>	
Cryptographic Formula Obfuscation	208
<i>Giovanni Di Crescenzo</i>	
Fault Analysis of the New Ukrainian Hash Function Standard: Kupyna	225
<i>Onur Duman and Amr Youssef</i>	

Cyber Physical Security and Hardware Security

When Fault Injection Collides with Hardware Complexity	243
<i>Sebanjila Kevin Bukasa, Ludovic Claudepierre, Ronan Lashermes, and Jean-Louis Lanet</i>	
A Study on Mitigation Techniques for SCADA-Driven Cyber-Physical Systems (Position Paper)	257
<i>Mariana Segovia, Ana Rosa Cavalli, Nora Cuppens, and Joaquin Garcia-Alfaro</i>	

Access Control

Mining Relationship-Based Access Control Policies from Incomplete and Noisy Data.	267
<i>Thang Bui, Scott D. Stoller, and Jiajie Li</i>	
Fine-Grained Access Control for Microservices.	285
<i>Antonio Nehme, Vitor Jesus, Khaled Mahbub, and Ali Abdallah</i>	

Achieving Mobile-Health Privacy Using Attribute-Based Access Control 301
Vignesh Pagadala and Indrakshi Ray

Author Index 317