Lecture Notes in Computer Science 11358

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

Springer

Editors
Nur Zincir-Heywood
Dalhousie University
Halifax, NS, Canada

Guillaume Bonfante
École des Mines de Nancy
Nancy, France

Mourad Debbabi
Concordia University
Montreal, QC, Canada

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

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 Autonoma 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 Stakhanova	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 Conccordia, 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
Guang Gong

Privacy and Ethical Challenges in Big Data 17
Sébastien Gambs

Mobile Security

Decentralized Dynamic Security Enforcement for Mobile Applications with CliSeAuDroid 29
Tobias Hamann and Heiko Mantel

Mobile Travel Credentials 46
David Bissessar, Maryam Hezaveh, Fayzah Alshammari, and Carlisle Adams

Cloud Security and Big Data

Cloud Security Auditing: Major Approaches and Existing Challenges 61
Suryadipta Majumdar, Taous Madi, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi

Secure Joins with MapReduce 78
Xavier Bultel, Radu Ciucanu, Matthieu Giraud, Pascal Lafourcade, and Lihua Ye

Daedalus: Network Anomaly Detection on IDS Stream Logs 95
Aniss Chohra, Mourad Debbabi, and Paria Shirani

IoT Security

Configuring Data Flows in the Internet of Things for Security and Privacy Requirements 115
Luigi Logrippo and Abdelouadoud Stambouli

Validating Requirements of Access Control for Cloud-Edge IoT Solutions (Short Paper) 131
Tahir Ahmad and Silvio Ranise

Software Security, Malware Analysis, and Vulnerability Detection

Evading Deep Neural Network and Random Forest Classifiers by Generating Adversarial Samples 143
Erick Eduardo Bernal Martinez, Bella Oh, Feng Li, and Xiao Luo

Protection of Systems Against Fuzzing Attacks 156
Léopold Ouairy, Hélène Le-Bouder, and Jean-Louis Lanet

A Comparative Study Across Static and Dynamic Side-Channel Countermeasures 173
Yuri Gil Dantas, Tobias Hamann, and Heiko Mantel

Cryptography

Card-Based Cryptographic Protocols with the Minimum Number of Cards Using Private Operations 193
Hibiki Ono and Yoshifumi Manabe

Cryptographic Formula Obfuscation 208
Giovanni Di Crescenzo

Fault Analysis of the New Ukrainian Hash Function Standard: Kupyna 225
Onur Duman and Amr Youssef

Cyber Physical Security and Hardware Security

When Fault Injection Collides with Hardware Complexity 243
Sebanjila Kevin Bukasa, Ludovic Claudepierre, Ronan Lashermes, and Jean-Louis Lanet

A Study on Mitigation Techniques for SCADA-Driven Cyber-Physical Systems (Position Paper) 257
Mariana Segovia, Ana Rosa Cavalli, Nora Cuppens, and Joaquin Garcia-Alfaro

Access Control

Mining Relationship-Based Access Control Policies from Incomplete and Noisy Data 267
Thang Bui, Scott D. Stoller, and Jiajie Li

Fine-Grained Access Control for Microservices 285
Antonio Nehme, Vitor Jesus, Khaled Mahbub, and Ali Abdallah

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

Author Index 317