

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, 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/7410>

Frédéric Cuppens · Lingyu Wang
Nora Cuppens-Boulahia · Nadia Tawbi
Joaquin Garcia-Alfaro (Eds.)

Foundations and Practice of Security

9th International Symposium, FPS 2016
Québec City, QC, Canada, October 24–25, 2016
Revised Selected Papers

Editors

Frédéric Cuppens
Télécom Bretagne
Cesson Sévigné
France

Lingyu Wang
Concordia Inst for Info
Concordia University
Montreal, QC
Canada

Nora Cuppens-Boulahia
Cesson-Sevigne
Télécom Bretagne
Cesson Sévigné
France

Nadia Tawbi
Local 3950, pavillon Adrien Pouliot
Université Laval
Quebec, QC
Canada

Joaquin Garcia-Alfaro
Télécom SudParis
Evry
France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-51965-4

ISBN 978-3-319-51966-1 (eBook)

DOI 10.1007/978-3-319-51966-1

Library of Congress Control Number: 2016961700

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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 Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 9th International Symposium on Foundations and Practice of Security (FPS 2016), which was hosted by Université Laval, Québec City, Quebec, Canada, during October 24–26, 2016. Each submission was reviewed by at least three committee members. The review process was followed by intensive discussions over a period of one week. The Program Committee selected 18 regular papers and five short papers for presentation. The accepted papers cover diverse research themes, ranging from classic topics, such as malware, anomaly detection, and privacy, to emerging issues, such as security and privacy in mobile computing and cloud. The program was completed with three excellent invited talks given by François Laviolette (Université Laval), Jean-Yves Marion (Lorraine University, France), and Jeremy Clark (Concordia University).

Many people contributed to the success of FPS 2016. 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 volunteered to read and discuss the papers. We greatly thank the local Organizing Committee, Josée Desharnais and Andrew Bedford, for their great efforts to organize and perfectly control the logistics during the symposium. We also want to express our gratitude to the publication chair, Joaquin Garcia-Alfaro (Télécom SudParis), for his work in editing the proceedings. Last but not least, thanks to all the attendees. As security becomes an essential property in information and communication technologies, there is a growing need to develop efficient methods to analyze and design systems providing a high level of security and privacy. We hope the articles in this proceedings volume will be valuable for your professional activities in this area.

November 2016

Nora Cuppens-Boulahia
Frédéric Cuppens
Nadia Tawbi
Lingyu Wang

Organization

General Chairs

Nadia Tawbi
Nora Cuppens-Boulahia

Université Laval, Canada
Télécom Bretagne, France

Program Co-chairs

Lingyu Wang
Frédéric Cuppens

Concordia University, Canada
Télécom Bretagne, France

Publications Chair

Joaquin Garcia-Alfaro

Télécom SudParis, France

Local Organizing Committee

Nadia Tawbi
Josée Desharnais
Andrew Bedford

Université Laval, Canada
Université Laval, Canada
Université Laval, Canada

Publicity Chair

Raphaël Khoury

Université du Québec à Chicoutimi, Canada

Program Committee

Esma Aimeur
Samiha Ayed
Jordi Castella-Roca
Frédéric Cuppens
Nora Cuppens-Boulahia
Mila Dalla Preda
Jean-Luc Danger
Mourad Debbabi
Josée Desharnais
Nicola Dragoni
Martin Gagné
Sebastien Gambs
Joaquin Garcia-Alfaro
Jordi Herrera-Joancomarti

Université de Montréal, Canada
Télécom Bretagne, France
Rovira i Virgili University, Spain
Télécom Bretagne, France
Télécom Bretagne, France
University of Verona, Italy
Télécom ParisTech, France
Concordia University, Canada
Université Laval, Canada
Technical University of Denmark, Denmark
Wheaton College, USA
Université du Québec à Montréal, Canada
Télécom SudParis, France
Autonomous University of Barcelona, Spain

Chunfu Jia	Nankai University, People's Republic of China
Bruce Kapron	University of Victoria, Canada
Raphaël Khoury	Université du Québec à Chicoutimi, Canada
Hyoungshick Kim	Sungkyunkwan University, South Korea
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	University of Auvergne, France
Giovanni Livraga	University of Milan, Italy
Luigi Logrippo	Université du Québec en Outaouais, Canada
Flaminia Luccio	Ca'Foscari University of Venice, Italy
Ilaria Matteucci	Istituto di Informatica e Telematica, Italy
Mohamed Mejri	Université Laval, Canada
Guillermo Navarro-Arribas	Autonomous University of Barcelona, Spain
Jordi Nin	Universitat Politècnica de Catalunya, Spain
Melek Önen	Eurecom, France
Andreas Pashalidis	Bundesamt für Sicherheit in der Informationstechnik, Germany
Marie-Laure Potet	Ensimag, France
Silvio Ranise	FBK, Security and Trust Unit, Italy
Andrea Saracino	Università di Pisa, Italy
Claudio Soriente	Telefonica Research and Development, Spain
Chamseddine Talhi	Ecole de Technologie Supérieure Montréal, Canada
Nadia Tawbi	Université Laval, Canada
Alexandre Viejo	Rovira i Virgili University, Spain
Lingyu Wang	Concordia University, Canada
Lena Wiese	Göttingen University, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands
Nur Zincir Heywood	Dalhousie University, Canada
Mohammad Zulkernine	Queen's University, Canada

Additional Reviewers

Naofumi Homma	Tohoku University, Japan
Omer Yuksel	Eindhoven University of Technology, The Netherlands
Taos Madi	Concordia University, Canada
Maxime Puy	University of Grenoble, France
Stéphane Devismes	University of Grenoble, France
Davide Fauri	Eindhoven University of Technology, The Netherlands
Saed Alrabaee	Concordia University, Canada
Riccardo Focardi	Ca'Foscari University of Venice, Italy
Shahrear Iqbal	Queen's University, Canada
Suryadiptra Majumdar	Concordia University, Canada
Feras Aljumah	Concordia University, Canada
Andrew Bedford	Université Laval, Canada
Mahdi Alizadeh	Eindhoven University of Technology, The Netherlands

Steering Committee

Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Mourad Debbabi	University of Concordia, Canada
Joaquin Garcia-Alfaro	Télécom SudParis, France
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	University of 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

Malware and Anomaly Detection

MalProfiler: Automatic and Effective Classification of Android Malicious Apps in Behavioral Classes	3
<i>Antonio La Marra, Fabio Martinelli, Andrea Saracino, and Mina Sheikhalishahi</i>	
ANDRANA: Quick and Accurate Malware Detection for Android.	20
<i>Andrew Bedford, Sébastien Garvin, Josée Desharnais, Nadia Tawbi, Hana Ajakan, Frédéric Audet, and Bernard Lebel</i>	
Micro-signatures: The Effectiveness of Known Bad N-Grams for Network Anomaly Detection	36
<i>Richard Harang and Peter Mell</i>	

Intrusion Response

Multi-Criteria Recommender Approach for Supporting Intrusion Response System	51
<i>Tarek Bouyahia, Nora Cuppens-Boulahia, Frédéric Cuppens, and Fabien Autrel</i>	
An Optimal Metric-Aware Response Selection Strategy for Intrusion Response Systems.	68
<i>Nadine Herold, Matthias Wachs, Stephan-A. Posselt, and Georg Carle</i>	
Attack Mitigation by Data Structure Randomization	85
<i>Zhongtian Chen and Hao Han</i>	

Vulnerability Analysis and Security Metrics

Vulnerability Analysis of Software Defined Networking.	97
<i>Salaheddine Zerkane, David Espes, Philippe Le Parc, and Frédéric Cuppens</i>	
Towards Metric-Driven, Application-Specific Visualization of Attack Graphs.	117
<i>Mickael Emirkanian-Bouchard and Lingyu Wang</i>	
Insider Threat Likelihood Assessment for Access Control Systems: Quantitative Approach	135
<i>Sofiene Boulares, Kamel Adi, and Luigi Logrippo</i>	

Privacy and Verification

An Enhancement of Privacy-Preserving Wildcards Pattern Matching	145
<i>Tushar Kanti Saha and Takeshi Koshiba</i>	
Privacy-Aware Data Sharing in a Tree-Based Categorical Clustering Algorithm	161
<i>Mina Sheikhalishahi, Mohamed Mejri, Nadia Tawbi, and Fabio Martinelli</i>	
Three Views of Log Trace Triaging	179
<i>Raphaël Khoury, Sébastien Gaboury, and Sylvain Hallé</i>	

Crypto and Communication Security

A Multi-round Side Channel Attack on AES Using Belief Propagation	199
<i>Hélène Le Boudier, Ronan Lashermes, Yanis Linge, Gaël Thomas, and Jean-Yves Zie</i>	
Anonymizable Ring Signature Without Pairing	214
<i>Olivier Blazy, Xavier Bultel, and Pascal Lafourcade</i>	
Security Analysis of WirelessHART Communication Scheme	223
<i>Lyes Bayou, David Espes, Nora Cuppens-Boulahia, and Frédéric Cuppens</i>	

Malware and Antivirus

Function Classification for the Retro-Engineering of Malwares	241
<i>Guillaume Bonfante and Julien Oury Nogues</i>	
On the Feasibility of Malware Authorship Attribution	256
<i>Saed Alrabaa, Paria Shirani, Mourad Debbabi, and Lingyu Wang</i>	
Semantically Non-preserving Transformations for Antivirus Evaluation	273
<i>Erkan Ersan, Lior Malka, and Bruce M. Kapron</i>	

Web, Cloud, and Delegation

A Self-correcting Information Flow Control Model for the Web-Browser	285
<i>Deepak Subramanian, Guillaume Hiet, and Christophe Bidan</i>	
Threat Modeling for Cloud Data Center Infrastructures	302
<i>Nawaf Alhebaishi, Lingyu Wang, Sushil Jajodia, and Anoop Singhal</i>	

Strategies for Incorporating Delegation into Attribute-Based Access Control (ABAC).	320
<i>Daniel Servos and Sylvia L. Osborn</i>	

Physical Security

Patrolling Trees with Mobile Robots	331
<i>Jurek Czyzowicz, Adrian Kosowski, Evangelos Kranakis, and Najmeh Taleb</i>	

Towards Side-Channel Secure Firmware Updates: A Minimalist Anomaly Detection Approach.	345
<i>Oscar M. Guillen, Fabrizio De Santis, Ralf Brederlow, and Georg Sigl</i>	

Author Index	361
-------------------------------	-----