

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA


More information about this series at <http://www.springer.com/series/7410>

Jianying Zhou · Robert Deng ·
Zhou Li · Suryadipta Majumdar ·
Weizhi Meng · Lingyu Wang ·
Kehuan Zhang (Eds.)

Applied Cryptography and Network Security Workshops

ACNS 2019 Satellite Workshops, SiMLA, Cloud S&P, AIBlock, and AIoTS
Bogota, Colombia, June 5–7, 2019
Proceedings

Editors


Jiaying Zhou 
Singapore University of Technology
and Design
Singapore, Singapore

Zhou Li
University of California
Irvine, USA

Weizhi Meng 
Technical University of Denmark
Kongens Lyngby, Denmark

Kehuan Zhang
Chinese University of Hong Kong
Shatin, Hong Kong

Robert Deng
Singapore Management University
Singapore, Singapore

Suryadipta Majumdar 
Massry Center for Business
University at Albany-SUNY
Albany, NY, USA

Lingyu Wang 
Concordia University
Montreal, QC, Canada

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-29728-2

ISBN 978-3-030-29729-9 (eBook)

<https://doi.org/10.1007/978-3-030-29729-9>

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 post-proceedings contains the papers selected for presentation at ACNS 2019 satellite workshops, which were held in conjunction with the main conference (the 17th International Conference on Applied Cryptography and Network Security) during June 5–7, 2019, in Bogota, Colombia. The local organization was in the capable hands of Professors Valerie Gauthier-Umana from Universidad del Rosario, Colombia, and Martin Ochoa, Universidad del Rosario and Cyxtera Technologies; we are deeply indebted to them for their generous support and leadership to ensure the success of the event.

It was a new initiative for ACNS to set up satellite workshops in 2019. Each workshop provided a forum to address a specific topic at the forefront of cybersecurity research. In response to this year's call for workshop proposals, the following five workshops were launched.

- AIBlock – First International Workshop on Application Intelligence and Block-chain Security
- AIoTS – First International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security
- Cloud S&P – First International Workshop on Cloud Security and Privacy
- PriDA – First International Workshop on Privacy-preserving Distributed Data Analysis
- SiMLA – First International Workshop on Security in Machine Learning and its Applications

This year, we received a total of 30 submissions. Each workshop had its own Program Committee (PC) in charge of the review process. These papers were evaluated on the basis of their significance, novelty, and technical quality. The review process was double-blind. In the end, 10 papers were selected for presentation at four workshops (PriDA was canceled), with an acceptance rate of 33%. The following paper received the ACNS 2019 Best Workshop Paper Award.

- “Risk-based Static Authentication in Web Applications with Behavioural Biometrics and Session Context Analytics,” by Jesus Solano, Luis Camacho, Alejandro Correa, Claudio Deiro, Javier Vargas, and Martin Ochoa.

A couple of papers from the post-proceedings will be nominated for submission of an extended version to a special issue in the *International Journal of Information Security* published by Springer.

ACNS 2019 workshops were made possible by the joint efforts of many individuals and organizations. We appreciate Springer's strong support on our new initiative. We sincerely thank the authors of all submissions. We are grateful to the program chairs and PC members of each workshop for their great effort in providing professional reviews and interesting feedback to authors in a tight time schedule. We thank all the

external reviewers for assisting the PC in their particular areas of expertise. We also thank the organizing team members of the main conference as well as each workshop for their help in various aspects.

Last but not least, we thank everyone else, speakers and session chairs, for their contribution to the program of ACNS 2019 workshops.

We believe this is a good start for the success of ACNS satellite workshops. We hope the existing workshops will keep growing and new workshops on emerging topics will be launched in the coming years. We expect it could provide a stimulating platform to discuss open problems at the forefront of cybersecurity research.

July 2019

Jianying Zhou
ACNS 2019 Workshop Chair

SiMLA 2019

First International Workshop on Security in Machine Learning and its Applications

**Bogota, Colombia
June 5, 2019**

Program Chairs

Zhou Li	University of California Irvine, USA
Kehuan Zhang	The Chinese University of Hong Kong, SAR China

Program Committee

Ninghui Li	Purdue University, USA
Yinqian Zhang	Ohio State University, USA
Di Tang	The Chinese University of Hong Kong, SAR China
Xiaokui Shu	IBM, USA
Jialong Zhang	ByteDance AI Lab, USA
Mohammad Al Faruque	University of California Irvine, USA
Xiapu Daniel Luo	The Hong Kong Polytechnic University, SAR China
Kai Chen	Institute of Information Engineering, Chinese Academy of Science, China
Zhe Zhou	Fudan University, China

Additional Reviewers

Guo, Zhixiu
Lu, Haochuan
Tan, Mingtian
Yuan, Xuejing

CLOUD S&P 2019

First International Workshop on Cloud Security and Privacy

Bogota, Colombia

June 5, 2019

Program Chairs

Suryadipta Majumdar
Lingyu Wang

University at Albany, USA
Concordia University, Canada

Web Chair

Sudershan L T

Concordia University, Canada

Program Committee

Vijay Atluri
Mauro Conti
Sabrina De Capitani di
Vimercati

Rutgers University, USA
University of Padua, Italy
Università degli studi di Milano, Italy

Sara Foresti
Xinwen Fu
Yuan Hong
Patrick Hung
Yosr Jarraya
Ram Krishnan
Zheli Liu
Rongxing Lu
Ali Miri

Università degli Studi di Milano, Italy
University of Central Florida, USA
Illinois Institute of Technology, USA
University of Ontario Institute of Technology, Canada
Ericsson Security, Canada
University of Texas at San Antonio, USA
Nankai University, China
University of New Brunswick, Canada
Ryerson University, Canada

Makan Pourzandi
Indrakshi Ray
Pierangela Samarati
Vijay Varadharajan
Mohammad Zulkernine

Ericsson Security, Canada
Colorado State University, USA
Università degli studi di Milano, Italy
University of Newcastle, Australia
Queen's University, Canada

Additional Reviewers

Karmakar, Kallol Krishna
Shojafar, Mohammad
Zhang, Mengyuan

AIBlock 2019

First International Workshop on Application Intelligence and Blockchain Security

Bogota, Colombia

June 5, 2019

Program Chairs

Weizhi Meng
Zhiqiang Liu
Chunhua Su

Technical University of Denmark, Denmark
Shanghai Jiao Tong University, China
University of Aizu, Japan

Program Committee

Ashiq Anjum
Man Ho Au
Raja Naeem Akram
David Chadwick
Konstantinos Chalkias
Taolue Chen
Dieter Gollmann
Debiao He
Georgios Kambourakis
Hyoungshick Kim
Hiroaki Kikuchi
Peter Lewis
Jiqiang Lu
Xiapu Luo
Felix Gomez Marmol
Petr Novotny
Jun Shao
Seungwon Shin
Paolo Tasca
Andreas Veneris
Qianhong Wu

University of Derby, UK
The Hong Kong Polytechnic University, SAR China
Royal Holloway, University of London, UK
University of Kent, UK
R3, UK and USA
Oxford University, UK
Hamburg University of Technology, Germany
Wuhan University, China
University of the Aegean, Greece
Sungkyunkwan University, South Korea
Meiji University, Japan
Aston University, UK
Beihang University, China
The Hong Kong Polytechnic University, SAR China
University of Murcia, Spain
IBM, USA
Zhejiang Gongshang University, China
KAIST, South Korea
University College London, UK
University of Toronto, Canada
Beihang University, China

Additional Reviewers

Dai, Xiaopeng
Recchia, Alessandro
Wu, Lei

AIoTS 2019

First International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security

**Bagota, Colombia
June 5, 2019**

Program Chairs

Robert Deng	Singapore Management University, Singapore
Sandra Rueda	Universidad de los Andes, Colombia

Organizing Chairs

Sridhar Adepu	SUTD, Singapore
John Henry Castellanos	SUTD, Singapore
Chuadhry Mujeeb Ahmed	SUTD, Singapore

Publicity Chair

Robert Kooij	SUTD, Singapore
--------------	-----------------

Program Committee

Alvaro Cardenas	University of California Santa Cruz, USA
Ee-Chien Chang	National University of Singapore, Singapore
Debin Gao	Singapore Management University, Singapore
Luis Garcia	University of California Los Angeles, USA
Dieter Gollmann	TU Hamburg, Germany
Pieter Hartel	TU Delft, The Netherlands
Eunsuk Kang	Carnegie Mellon University, USA
Junyu Lai	UESTC, China
Elena Lisova	Malardalen University, Sweden
Javier Lopez	University of Malaga, Spain
Di Ma	University of Michigan, USA
Chris Poskitt	SUTD, Singapore
Pandu Rangan	IIT Madras, India
Rajib Ranjan Maiti	BITS-Hyderabad, India
Giedre Sabaliauskaite	SUTD, Singapore

Phani Vadrevu
Yousheng Zhou

University of New Orleans, USA
CQUPT, China

Additional Reviewers

Adepu, Sridhar
Ahmed, Chuadhry Mujeeb

Contents

SiMLA - Security in Machine Learning and its Applications

Risk-Based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics	3
<i>Jesus Solano, Luis Camacho, Alejandro Correa, Claudio Deiro, Javier Vargas, and Martín Ochoa</i>	
Using Honeypots in a Decentralized Framework to Defend Against Adversarial Machine-Learning Attacks.	24
<i>Fadi Younis and Ali Miri</i>	

Cloud S&P - Cloud Security and Privacy

Graphene: A Secure Cloud Communication Architecture	51
<i>Abu Faisal and Mohammad Zulkernine</i>	
A Survey on Machine Learning Applications for Software Defined Network Security	70
<i>Juliana Arevalo Herrera and Jorge E. Camargo</i>	

AIBlock - Application Intelligence and Blockchain Security

A New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations	97
<i>Jintai Ding</i>	
BSIEM-IoT: A Blockchain-Based and Distributed SIEM for the Internet of Things	108
<i>Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel Díaz López, and Félix Gómez Mármol</i>	
Towards Blockchain Challenge-Based Collaborative Intrusion Detection . . .	122
<i>Wenjuan Li, Yu Wang, Jin Li, and Man Ho Au</i>	

AIoTS - Artificial Intelligence and Industrial Internet-of-Things Security

Enhancement to the Privacy-Aware Authentication for Wi-Fi Based Indoor Positioning Systems	143
<i>Jhonattan J. Barriga A., Sang Guun Yoo, and Juan Carlos Polo</i>	

Design of a FDIA Resilient Protection Scheme for Power Networks
by Securing Minimal Sensor Set 156
Tanmoy Kanti Das, Subhojit Ghosh, Ebha Koley, and Jianying Zhou

Strong Leakage Resilient Encryption by Hiding Partial Ciphertext. 172
Jia Xu and Jianying Zhou

Author Index 193