

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 · Mauro Conti ·
Chuadhry Mujeeb Ahmed ·
Man Ho Au · Lejla Batina ·
Zhou Li · Jingqiang Lin ·
Eleonora Losiouk · Bo Luo ·
Suryadipta Majumdar · Weizhi Meng ·
Martín Ochoa · Stjepan Picek ·
Georgios Portokalidis · Cong Wang ·
Kehuan Zhang (Eds.)

Applied Cryptography and Network Security Workshops

ACNS 2020 Satellite Workshops
AIBlock, AIHWS, AIoTS, Cloud S&P, SCI, SecMT, and SiMLA
Rome, Italy, October 19–22, 2020
Proceedings

Editors

Jianying Zhou 
Singapore University of Technology
and Design
Singapore, Singapore

Chuadhry Mujeeb Ahmed 
Singapore University of Technology
and Design
Singapore, Singapore

Lejla Batina 
ICIS
Radboud University Nijmegen
Nijmegen, The Netherlands

Jingqiang Lin
University of Science and Technology
of China
Hefei, China


Bo Luo
University of Kansas
Lawrence, KS, USA

Weizhi Meng 
Technical University of Denmark
Lyngby, Denmark


Stjepan Picek 
Delft University of Technology
Delft, The Netherlands


Cong Wang 
City University of Hong Kong
Hong Kong, China


Mauro Conti 
University of Padua
Padua, Italy


Man Ho Au 
The University of Hong Kong
Hong Kong, Hong Kong

Zhou Li
University of California
Irvine, CA, USA

Eleonora Losiouk 
University of Padua
Padua, Italy

Suryadipta Majumdar 
CIISE
Concordia University
Montréal, QC, Canada

Martín Ochoa 
AppGate Inc.
Bogotá, Colombia

Georgios Portokalidis 
Stevens Institute of Technology
Hoboken, NJ, USA

Kehuan Zhang
Chinese University of Hong Kong
Shatin, Hong Kong

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-61637-3 ISBN 978-3-030-61638-0 (eBook)
<https://doi.org/10.1007/978-3-030-61638-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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

These proceedings contain the papers selected for presentation at the 18th International Conference on Applied Cryptography and Network Security (ACNS 2020) satellite workshops, which were held in parallel with the main conference.

ACNS 2020 was planned to be held in Rome, Italy, during June 22–25 2020. Due to the unexpected COVID-19 crisis, we first postponed the conference to October 19–22, 2020, but ended up deciding for the safety of all participants to have a virtual conference. The local organization was in the capable hands of Emiliano Casalicchio and Angelo Spognardi (Sapienza University of Rome, Italy) and Giuseppe Bernieri (University of Padua, Italy) as general co-chairs, and Massimo Bernaschi (CNR, Italy) as organizing chair. We are deeply indebted to them for their tireless work to ensure the success of the conference even in such complex conditions.

ACNS initiated four satellite workshops successfully 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, three new workshops were launched besides the four workshops launched last year.

- AIBlock: Second ACNS Workshop on Application Intelligence and Blockchain Security
- AIHWS: First ACNS Workshop on Artificial Intelligence in Hardware Security
- AIoTS: Second ACNS Workshop on Artificial Intelligence and Industrial IoT Security
- Cloud S&P: Second ACNS Workshop on Cloud Security and Privacy
- SCI: First ACNS Workshop on Secure Cryptographic Implementation
- SecMT: First ACNS Workshop on Security in Mobile Technologies
- SiMLA: Second ACNS Workshop on Security in Machine Learning and its Applications

This year, we received a total of 65 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, 31 papers were selected for presentation at seven workshops, with an acceptance rate of 47.7%.

ACNS also gave the best workshop paper award. The winning papers were selected from the nominated candidate papers from each workshop. The following two papers shared ACNS 2020 Best Workshop Paper Award:

- Michael McCoyd, Won Park, Steven Chen, Neil Shah, Ryan Roggenkemper, Minjune Hwang, Xinyu Liu, and David Wagner, “Minority Reports Defense: Defending Against Adversarial Patches,” from the SiMLA workshop
- Valence Cristiani, Maxime Lecomte, and Philippe Maurine, “Leakage Assessment through Neural Estimation of the Mutual Information,” from the AIHWS workshop

Besides the regular papers being presented at the workshops, there were also six invited talks.

- “Computing on Encrypted Data: Hardware to the Rescue” by Farinaz Koushanfar from UC San Diego, USA, and “Fooling Smart Machines: Security Challenges for Machine Learning” by Simon Friedberger from NXP, The Netherlands, at the AIHWS workshop
- “Adversarial Classification in IoT Applications Using Differential Privacy” by Alvaro Cardenas from University of California, Santa Cruz, USA, at the AIOIS workshop
- “Towards Building a Scalable Security Analytics Framework for Attack Detection on Ethereum” by Yajin Zhou from Zhejiang University, China, at the CLOUD S&P workshop
- “Cache-in-the-Middle (CITM) Attacks: Manipulating Sensitive Data in Isolated Execution Environments” by Kun Sun from George Mason University, USA, at the SCI workshop
- “Security and Privacy: The Sorrows of Young Droid” by Alessio Merlo from University of Genoa, Italy, at the SecMT workshop

ACNS 2020 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 2020 workshops.

We are glad to see the existing workshops are growing and new workshops on emerging topics are being launched. We hope this trend will continue in the coming years. We expect it could provide a stimulating platform to discuss open problems at the forefront of cybersecurity research.

September 2020

Jianying Zhou
Mauro Conti
ACNS 2020 Workshop Chairs

AIBlock 2020

Second ACNS Workshop on Application Intelligence and Blockchain Security

19 October 2020

General Chairs

Chunhua Su
Xiapu Luo

University of Aizu, Japan
The Hong Kong Polytechnic University, China

Program Chairs

Weizhi Meng
Man Ho Au

Technical University of Denmark, Denmark
The University of Hong Kong, China

Program Committee

Raja Naeem Akram
Jintai Ding
Dieter Gollmann
Debiao He
Qiong Huang
Georgios Kambourakis
Chhagan Lal
Romain Laborde
Wenjuan Li
Jiqiang Lu
Felix Gomez Marmol
Pantaleone Nespoli
Jun Shao
Jiangang Shu
Andreas Veneris
Qianhong Wu
Ding Wang
Guomin Yang

Royal Holloway, University of London, UK
University of Cincinnati, USA
Hamburg University of Technology, Germany
Wuhan University, China
South China Agricultural University, China
University of the Aegean, Greece
University of Padua, Italy
Paul Sabatier University, France
The Hong Kong Polytechnic University, China
Beihang University, China
University of Murcia, Spain
University of Murcia, Spain
Zhejiang Gongshang University, China
Peng Cheng Laboratory, China
University of Toronto, Canada
Beihang University, China
Nankai University, China
University of Wollongong, Australia

Additional Reviewers

Gu, Zhiqiang
Luo, Zhenqiu
Miao, Ying
Wang, Chenyu

AIHWS 2020

First ACNS Workshop on Artificial Intelligence in Hardware Security

21 October 2020

Program Chairs

Lejla Batina
Stjepan Picek

Radboud University, The Netherlands
Delft University of Technology, The Netherlands

Program Committee

Lex Schoonen
Fateme Ganji
Liran Lerman
Shahin Tajik
Lukasz Chmielewski
Vincent Verneuil
Alan Jovic
Luca Mariot
Chitchanok

BrightSight, The Netherlands
Worcester Polytechnic Institute, USA
Thales Belgium, Belgium
Worcester Polytechnic Institute, USA
Riscure, The Netherlands
NXP Semiconductors, Germany
University of Zagreb, Croatia
Delft University of Technology, The Netherlands
The University of Adelaide, Australia

Chuengsatiansup
Nele Mentens
Dirmanto Jap
Shivam Bhasin
Nikita Veshchikov
Kostas Papagiannopoulos
Guilherme Perin

Katholieke Universiteit Leuven, Belgium
Nanyang Technological University, Singapore
Nanyang Technological University, Singapore
NXP, Belgium
NXP, Germany
Delft University of Technology, The Netherlands

Publicity Chair

Marina Krcek

Delft University of Technology, The Netherlands

AIoTS 2020

Second ACNS Workshop on Artificial Intelligence and Industrial IoT Security

20 October 2020

Program Chairs

Martin Ochoa	Cyxtera, Colombia
Chuahdhy Mujeeb Ahmed	SUTD, Singapore

Organizing Chairs

Sridhar Adepu	SUTD, Singapore
John Henry Castellanos	SUTD, Singapore

Publicity Chair

Chhagan Lal	University of Padua, Italy
-------------	----------------------------

Program Committee

Anand Agrawal	NYU Abu Dhabi, UAE
Alvaro Cardenas	University of California, Santa Cruz, USA
Ding Ding	George Washington University, USA
Luis Garcia	University of California, Los Angeles, USA
Amrita Ghosal	University of Padua, Italy
Venkata Reddy	IIPe-Visakhapatnam, India
Subir Halder	University of Padua, Italy
Nandha Kumar Kandasamy	SUTD, Singapore
Eunsuk Kang	Carnegie Mellon University, USA
Elena Lisova	Mälardalen University, Sweden
Chhagan Lal	University of Padua, Italy
Junyu Lai	UESTC, China
Eleonora Losiouk	University of Padua, Italy
Chris Poskitt	SMU, Singapore
Rajib Ranjan Maiti	BITS-Hyderabad, India
Tohid Shekari	Georgia Tech, USA
Federico Turrin	University of Padua, Italy
Riccardo Taormina	Delft University of Technology, The Netherlands
Robin Verma	UTSA, USA

Cloud S&P 2020

Second ACNS Workshop on Cloud Security and Privacy

22 October 2020

Program Chairs

Suryadipta Majumdar
Cong Wang

University at Albany, SUNY, USA
City University of Hong Kong, China

Program Committee

Daniel Bastos	British Telecom, UK
Helei Cui	Northwestern Polytechnical University, China
Nora Cuppens	IMT Atlantique, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Yosr Jarraya	Ericsson Security, Canada
Kallol Krishna Karmaker	The University of Newcastle, Australia
Eduard Marin	University of Birmingham, UK
Ali Miri	Ryerson University, Canada
Makan Pourzandi	Ericsson Security, Canada
Indrakshi Ray	Colorado State University, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Paria Shirani	Concordia University, Canada
Lingyu Wang	Concordia University, Canada
Xingliang Yuan	Monash University, Australia
Yifeng Zheng	Data61, CSIRO, Australia

Additional Reviewers

Shirazi, Hossein
Karanfil, Mark
Cabana, Olivier

SCI 2020

First ACNS Workshop on Secure Cryptographic Implementation

21 October 2020

Program Chairs

Jingqiang Lin
Bo Luo

University of Science and Technology of China, China
The University of Kansas, USA

Publication Chair

Jun Shao

Zhejiang Gongshang University, China

Publicity Chairs

Le Guan
Debiao He

University of Georgia, USA
Wuhan University, China

Web Chair

Yuan Ma

Chinese Academy of Sciences, China

Program Committee

Bo Chen
Fu Chen
Junfeng Fan
Johann Großschädl
Le Guan
Debiao He
Linzhi Jiang
Fengjun Li
Xiao Liu
Zhe Liu

Michigan Technological University, USA
Central University of Finance and Economics, China
Open Security Research, Inc., China
University of Luxembourg, Luxembourg
University of Georgia, USA
Wuhan University, China
University of Surrey, UK
The University of Kansas, USA
Facebook Inc., USA
Nanjing University of Aeronautics and Astronautics,
China
Chinese Academy of Sciences, China
Zhejiang Gongshang University, China
Beijing University of Posts and Telecommunications,
China
Wuhan University, China
Stevens Institute of Technology, USA

Yuan Ma
Jun Shao
Ruisheng Shi

Juan Wang
Jun Xu

Li Yang	Xidian University, China
Fan Zhang	Zhejiang University, China
Fangyu Zheng	Chinese Academy of Sciences, China

Additional Reviewers

Qi Jiang	Xidian University, China
Weijing You	Chinese Academy of Sciences, China
Junwei Zhang	Xidian University, China

SecMT 2020

First ACNS Workshop on Security in Mobile Technologies

19 October 2020

Program Chairs

Eleonora Losiouk
Georgios Portokalidis

University of Padua, Italy
Stevens Institute of Technology, USA

General Chair

Olga Gadyatskaya

Leiden University, The Netherlands

Program Committee

Kevin Allix
Elias Athanasopoulos
Antonio Bianchi
Yanick Fratantonio
Li Li
Isabella Mastroeni
Guozhu Meng
Kaveh Razavi
Andrea Saracino
Flavio Toffalini

University of Luxembourg, Luxembourg
University of Cyprus, Cyprus
Purdue University, USA
EURECOM, France
Monash University, Australia
University of Verona, Italy
Nanyang Technological University, Singapore
ETH Zurich, Switzerland
National Research Council, Italy
SUTD, Singapore

SiMLA 2020

Second ACNS Workshop on Security in Machine Learning and its Applications

20 October 2020

Program Chairs

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

Program Committee

Kangkook Jee	The University of Texas at Dallas, USA
Baojun Liu	Tsinghua University, China
Wenrui Diao	Shandong University, China
Yinqian Zhang	The Ohio State University, USA
Di Tang	The Chinese University of Hong Kong, China
Zhe Zhou	Fudan University, China
Kai Chen	Institute of Information Engineering, Chinese Academy of Sciences, China
Chaowei Xiao	University of Michigan, USA

Additional Reviewers

Mingxuan Liu
Li Wang
Zhixiu Guo

Contents

AIBlock – Application Intelligence and Blockchain Security

Towards a Formally Verified Implementation of the MimbleWimble Cryptocurrency Protocol	3
<i>Gustavo Betarte, Maximiliano Cristiá, Carlos Luna, Adrián Silveira, and Dante Zanarini</i>	
Secure Management of IoT Devices Based on Blockchain Non-fungible Tokens and Physical Unclonable Functions	24
<i>Javier Arcenegui, Rosario Arjona, and Iluminada Baturone</i>	
Bitcoin Blockchain Steganographic Analysis	41
<i>Alexandre Augusto Giron, Jean Everson Martina, and Ricardo Custódio</i>	
Dynamic Group Key Agreement for Resource-constrained Devices Using Blockchains	58
<i>Yaşar Berkay Taçyıldız, Orhan Ermiş, Gürkan Gür, and Fatih Alagöz</i>	
Tokenization of Real Estate Using Blockchain Technology	77
<i>Ashutosh Gupta, Jash Rathod, Dhiren Patel, Jay Bothra, Sanket Shanbhag, and Tanmay Bhalerao</i>	

AIHWS – Artificial Intelligence in Hardware Security

Practical Side-Channel Based Model Extraction Attack on Tree-Based Machine Learning Algorithm	93
<i>Dirmanto Jap, Ville Yli-Mäyry, Akira Ito, Rei Ueno, Shivam Bhasin, and Naofumi Homma</i>	
Controlling the Deep Learning-Based Side-Channel Analysis: A Way to Leverage from Heuristics	106
<i>Servio Paguada, Unai Rioja, and Igor Armendariz</i>	
A Comparison of Weight Initializers in Deep Learning-Based Side-Channel Analysis.	126
<i>Huimin Li, Marina Krček, and Guilherme Perin</i>	
Leakage Assessment Through Neural Estimation of the Mutual Information	144
<i>Valence Cristiani, Maxime Lecomte, and Philippe Maurine</i>	

Evolvable Hardware Architectures on FPGA for Side-Channel Security	163
<i>Mansoureh Labafniya, Shahram Etemadi Borujeni, and Nele Mentens</i>	
Simple Electromagnetic Analysis Against Activation Functions of Deep Neural Networks	181
<i>Go Takato, Takeshi Sugawara, Kazuo Sakiyama, and Yang Li</i>	
Performance Analysis of Multilayer Perceptron in Profiling Side-Channel Analysis	198
<i>Léo Weissbart</i>	
The Forgotten Hyperparameter: Introducing Dilated Convolution for Boosting CNN-Based Side-Channel Attacks	217
<i>Servio Paguada and Igor Armendariz</i>	
 AIoTS – Artificial Intelligence and Industrial IoT Security	
ARM-AFL: Coverage-Guided Fuzzing Framework for ARM-Based IoT Devices	239
<i>Rong Fan, Jianfeng Pan, and Shaomang Huang</i>	
Post-exploitation and Persistence Techniques Against Programmable Logic Controller	255
<i>Andrei Bytes and Jianying Zhou</i>	
Investigation of Cyber Attacks on a Water Distribution System	274
<i>Sridhar Adepu, Venkata Reddy Palleti, Gyanendra Mishra, and Aditya Mathur</i>	
 Cloud S&P – Cloud Security and Privacy	
Computing Neural Networks with Homomorphic Encryption and Verifiable Computing	295
<i>Abbass Madi, Renaud Sirdey, and Oana Stan</i>	
Attribute-Based Symmetric Searchable Encryption.	318
<i>Hai-Van Dang, Amjad Ullah, Alexandros Bakas, and Antonis Michalas</i>	
Towards Inclusive Privacy Protections in the Cloud.	337
<i>Tanusree Sharma, Tian Wang, Carlo Di Giulio, and Masooda Bashir</i>	
A Study on Microarchitectural Covert Channel Vulnerabilities in Infrastructure-as-a-Service.	360
<i>Benjamin Semal, Konstantinos Markantonakis, Raja Naeem Akram, and Jan Kalbantner</i>	

SCI – Secure Cryptographic Implementation

On New Zero-Knowledge Proofs for Fully Anonymous Lattice-Based Group Signature Scheme with Verifier-Local Revocation	381
<i>Yanhua Zhang, Ximeng Liu, Yifeng Yin, Qikun Zhang, and Huiwen Jia</i>	
Proofs of Ownership on Encrypted Cloud Data via Intel SGX	400
<i>Weijing You and Bo Chen</i>	
On the Verification of Signed Messages.	417
<i>Bowen Xu, Xin Xu, Quanwei Cai, Wei Wang, and QiongXiao Wang</i>	
Applications and Developments of the Lattice Attack in Side Channel Attacks	435
<i>Ziqiang Ma, Bingyu Li, Quanwei Cai, and Jun Yang</i>	
Exploring the Security of Certificate Transparency in the Wild	453
<i>Bingyu Li, Fengjun Li, Ziqiang Ma, and Qianhong Wu</i>	

SecMT – Security in Mobile Technologies

<i>DaVinci</i> : Android App Analysis Beyond Frida via Dynamic System Call Instrumentation	473
<i>Alexander Druffel and Kris Heid</i>	
MobHide: App-Level Runtime Data Anonymization on Mobile	490
<i>Davide Caputo, Luca Verderame, and Alessio Merlo</i>	
Evaluation of the Adoption and Privacy Risks of Google Prompts.	508
<i>Christos Avraam and Elias Athanasopoulos</i>	
On the Evolution of Security Issues in Android App Versions	523
<i>Anatoli Kalysch, Joschua Schilling, and Tilo Müller</i>	

SiMLA – Security in Machine Learning and Its Applications

Unsupervised Labelling of Stolen Handwritten Digit Embeddings with Density Matching.	545
<i>Thomas Thebaud, Gaël Le Lan, and Anthony Larcher</i>	
Minority Reports Defense: Defending Against Adversarial Patches	564
<i>Michael McCoyd, Won Park, Steven Chen, Neil Shah, Ryan Roggenkemper, Minjune Hwang, Jason Xinyu Liu, and David Wagner</i>	
Author Index	583