

## 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>

Zhiqiang Lin · Charalampos Papamanthou ·  
Michalis Polychronakis (Eds.)

# Information Security

22nd International Conference, ISC 2019  
New York City, NY, USA, September 16–18, 2019  
Proceedings

*Editors*

Zhiqiang Lin  
The Ohio State University  
Columbus, OH, USA

Charalampos Papamanthou  
University of Maryland  
College Park, MD, USA

Michalis Polychronakis  
Stony Brook University  
Stony Brook, NY, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-30214-6

ISBN 978-3-030-30215-3 (eBook)

<https://doi.org/10.1007/978-3-030-30215-3>

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

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 22nd Information Security Conference (ISC 2019), which took place in New York City, USA, during September 16–18, 2019. ISC is an annual international conference covering research in theory and applications of information security. Both academic research with high relevance to real-world problems, as well as developments in industrial and technical frontiers fall within the scope of the conference.

The 22nd edition of ISC was organized by Stony Brook University and was held at the SUNY Global Center in Manhattan. Professor Michalis Polychronakis (Stony Brook University) served as the general chair, and Professors Zhiqiang Lin (Ohio State University) and Charalampos Papamanthou (University of Maryland) served as the program co-chairs. The Program Committee comprised 41 members from top institutions around the world. Out of 86 submissions, the Program Committee eventually selected 23 papers (8 of which were accepted after a shepherding process) for presentation in the conference and publication in the proceedings, resulting in an acceptance rate of 26.7%. The submission process was double-blind, and the review process was organized and managed through the HotCRP online reviewing system, with all papers receiving at least three reviews. The final program was quite balanced in terms of topics, containing both theoretical/cryptography papers, as well as more practical/systems security papers. Beyond the research papers, the conference program also included two insightful keynote talks by Professors Engin Kirda (Northeastern University) and Elaine Shi (Cornell), on advanced malware and consensus protocols, respectively.

A successful conference is the result of the joint effort of many people. We would like to express our appreciation to the Program Committee members and external reviewers for the time spent reviewing papers, participating in the online discussion, and shepherding some of the papers to ensure the highest quality possible. We also deeply thank the members of the Organizing Committee for their hard work in making ISC 2019 such a successful event, and our invited speakers for their willingness to participate in the conference. We are wholeheartedly thankful to our sponsors, Facebook and Springer, for generously supporting ISC 2019. We also thank Springer for publishing these proceedings as part of their LNCS series, and the ISC Steering Committee for their continuous support and assistance.

Finally, ISC 2019 would not have been possible without the authors who submitted their work and presented their contributions, as well as the attendees who came to the conference. We would like to thank them all, and we look forward to their future contributions to ISC.

July 2019

Zhiqiang Lin  
Charalampos Papamanthou  
Michalis Polychronakis

# Organization

## General Chair

Michalis Polychronakis

Stony Brook University, USA

## Program Chairs

Zhiqiang Lin

Ohio State University, USA

Charalampos (Babis)

University of Maryland, USA

Papamantou

## Publicity Chair

Cheng Huang

Sichuan University, China

## Organizing Committee

Kathy Germana

Stony Brook University, USA

Andrew Solar-Greco

Stony Brook University, USA

## Steering Committee

Ed Dawson

Queensland University of Technology, Australia

Javier Lopez

University of Malaga, Spain

Masahiro Mambo

Kanazawa University, Japan

Mark Manulis

University of Surrey, UK

Eiji Okamoto

University of Tsukuba, Japan

Michalis Polychronakis

Stony Brook University, USA

Susanne Wetzel

Stevens Institute of Technology, USA

Yuliang Zheng

University of Alabama at Birmingham, USA

Jianying Zhou

Singapore University of Technology and Design,  
Singapore

## Program Committee

Elias Athanasopoulos

University of Cyprus, Cyprus

Foteini Baldimtsi

George Mason University, USA

Alex Chepurnoy

IOHK, USA, and Ergo Platform, Russia

Sherman Chow

Chinese University of Hong Kong, SAR China

Dana Dachman-Soled

University of Maryland, USA

Lucas Davi

University of Duisburg-Essen, Germany

Brendan Dolan-Gavitt

New York University, USA

Sanjam Garg	UC Berkeley, USA
André Grégio	Federal University of Parana, Brazil
Esha Ghosh	Microsoft Research, USA
Alexandros Kapravelos	NC State University, USA
Vasileios Kemerlis	Brown University, USA
Evgenios Kornaropoulos	Brown University, USA
Alp Kupcu	Koc University, Turkey
Andrea Lanzi	University of Milan, Italy
Juanru Li	Shanghai Jiaotong University, China
Xiapu Luo	Hong Kong Polytechnic University, SAR China
Alex Malozemoff	Galois Inc., USA
Masahiro Mambo	Kanazawa University, Japan
Mark Manulis	University of Surrey, UK
Daniel Masny	Visa Research, USA
Kartik Nayak	VMware Research, USA
Nick Nikiforakis	Stony Brook University, USA
Dimitris Papadopoulos	HKUST, SAR China
Giancarlo Pellegrino	Stanford University, USA, and CISPA, Germany
Mike Reiter	University of North Carolina at Chapel Hill, USA
Brendan Saltaformaggio	Georgia Tech, USA
Roberto Tamassia	Brown University, USA
Nikos Triandopoulos	Stevens Institute of Technology, USA
Cong Wang	City University of Hong Kong, SAR China
Ding Wang	Peking University, China
Ruoyu (Fish) Wang	Arizona State University, USA
Xiao Wang	MIT and Boston University, USA
Xinyu Xing	Penn State University, USA
Arkady Yerukhimovich	George Washington University, USA
Yu Yu	Shanghai Jiaotong University, China
Moti Yung	Columbia University, USA
Yupeng Zhang	UC Berkeley, USA
Yajin Zhou	Zhejiang University, China
Jianying Zhou	Singapore University of Technology and Design, Singapore
Vassilis Zikas	University of Edinburgh, UK

## Sponsors

Facebook  
Stony Brook University

# Contents

## Attacks and Cryptanalysis

IBWH: An Intermittent Block Withholding Attack with Optimal Mining Reward Rate. . . . .	3
<i>Junming Ke, Pawel Szalachowski, Jianying Zhou, Qiuliang Xu, and Zheng Yang</i>	
Full Database Reconstruction with Access and Search Pattern Leakage . . . . .	25
<i>Evangelia Anna Markatou and Roberto Tamassia</i>	
Cube Cryptanalysis of Round-Reduced ACORN. . . . .	44
<i>Jingchun Yang, Meicheng Liu, and Dongdai Lin</i>	

## Crypto I: Secure Computation and Storage

Auditable Compressed Storage . . . . .	67
<i>Iraklis Leontiadis and Reza Curtmola</i>	
Decentralized Evaluation of Quadratic Polynomials on Encrypted Data . . . . .	87
<i>Chloé Héban, Duong Hieu Phan, and David Pointcheval</i>	
Robust Distributed Pseudorandom Functions for mNP Access Structures . . . . .	107
<i>Bei Liang and Aikaterini Mitrokotsa</i>	

## Machine Learning and Security

Can Today's Machine Learning Pass Image-Based Turing Tests? . . . . .	129
<i>Apostolis Zarras, Ilias Gerostathopoulos, and Daniel Méndez Fernández</i>	
PD-ML-Lite: Private Distributed Machine Learning from Lightweight Cryptography . . . . .	149
<i>Maksim Tsikhanovich, Malik Magdon-Ismail, Muhammad Ishaq, and Vassilis Zikas</i>	

## Crypto II: Zero-Knowledge Proofs

Code-Based Zero Knowledge PRF Arguments . . . . .	171
<i>Carlo Brunetta, Bei Liang, and Aikaterini Mitrokotsa</i>	
On New Zero-Knowledge Proofs for Lattice-Based Group Signatures with Verifier-Local Revocation . . . . .	190
<i>Yanhua Zhang, Yupu Hu, Qikun Zhang, and Huiwen Jia</i>	



## Defenses

When the Attacker Knows a Lot: The GAGA Graph Anonymizer . . . . .	211
<i>Arash Alavi, Rajiv Gupta, and Zhiyun Qian</i>	
Mitigation Techniques for Attacks on 1-Dimensional Databases that Support Range Queries . . . . .	231
<i>Evangelia Anna Markatou and Roberto Tamassia</i>	

## Web Security

Getting Under Alexa’s Umbrella: Infiltration Attacks Against Internet Top Domain Lists . . . . .	255
<i>Walter Rweyemamu, Tobias Lauinger, Christo Wilson, William Robertson, and Engin Kirda</i>	
Truth in Web Mining: Measuring the Profitability and the Imposed Overheads of Cryptojacking . . . . .	277
<i>Panagiotis Papadopoulos, Panagiotis Ilia, and Evangelos Markatos</i>	

## Side Channels

LightSense: A Novel Side Channel for Zero-permission Mobile User Tracking. . . . .	299
<i>Quanqi Ye, Yan Zhang, Guangdong Bai, Naipeng Dong, Zhenkai Liang, Jin Song Dong, and Haoyu Wang</i>	
Robust Covert Channels Based on DRAM Power Consumption . . . . .	319
<i>Thales Bandiera Paiva, Javier Navaridas, and Routo Terada</i>	

## Malware Analysis

Barnum: Detecting Document Malware via Control Flow Anomalies in Hardware Traces . . . . .	341
<i>Carter Yagemann, Salmin Sultana, Li Chen, and Wenke Lee</i>	
An Analysis of Malware Trends in Enterprise Networks . . . . .	360
<i>Abbas Acar, Long Lu, A. Selcuk Uluagac, and Engin Kirda</i>	
L(a)ying in (Test)Bed: How Biased Datasets Produce Impractical Results for Actual Malware Families’ Classification . . . . .	381
<i>Tamy Beppler, Marcus Botacin, Fabrício J. O. Ceschin, Luiz E. S. Oliveira, and André Grégio</i>	
Automated Reconstruction of Control Logic for Programmable Logic Controller Forensics . . . . .	402
<i>Syed Ali Qasim, Juan Lopez Jr., and Irfan Ahmed</i>	

Crypto III: Signatures and Authentication

Secure Stern Signatures in Quantum Random Oracle Model. . . . .	425
<i>Hanwen Feng, Jianwei Liu, and Qianhong Wu</i>	
Adding Linkability to Ring Signatures with One-Time Signatures. . . . .	445
<i>Xueli Wang, Yu Chen, and Xuecheng Ma</i>	
Cryptographic Authentication from the Iris. . . . .	465
<i>Sailesh Simhadri, James Steel, and Benjamin Fuller</i>	
Author Index . . . . .	487