Lecture Notes in Computer Science 12579

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

Stephan Krenn · Haya Shulman ·
Serge Vaudenay (Eds.)

Cryptology and Network Security

19th International Conference, CANS 2020 Vienna, Austria, December 14–16, 2020 Proceedings

Springer

Editors
Stephan Krenn
AIT Austrian Institute of Technology GmbH
Vienna, Austria

Haya Shulman
Fraunhofer SIT
Darmstadt, Germany

Serge Vaudenay
IC LASEC
EPFL
Lausanne, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-65410-8 ISBN 978-3-030-65411-5 (eBook)
https://doi.org/10.1007/978-3-030-65411-5

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

The 19th International Conference on Cryptology and Network Security (CANS 2020) was held during December 14–16, 2020, as an online conference, due to the COVID-19 pandemic. CANS 2020 was held in cooperation with the International Association for Cryptologic Research (IACR).

CANS is a recognized annual conference focusing on cryptology, computer and network security, and data security and privacy, attracting cutting-edge research findings from scientists around the world. Previous editions of CANS were held in Taipei ('01), San Francisco ('02), Miami ('03), Xiamen ('05), Suzhou ('06), Singapore ('07), Hong Kong ('08), Kanazawa ('09), Kuala Lumpur ('10), Sanya ('11), Darmstadt ('12), Parary ('13), Crete ('14), Marrakesh ('15), Milan ('16), Hong Kong ('17), Naples ('18), and Fuzhou ('19).

In 2020, the conference received 118 submissions. The submission and review process was done using the EasyChair Web-based software system. We were helped by 40 Program Committee members and 110 external reviewers. The submissions went through a doubly-anonymous review process and 30 papers were selected. This volume represents the revised version of the accepted papers.

Following the CANS tradition, the Program Committee awarded some authors. This year, the Best Paper Award was given for three papers:

- Daniel Kales and Greg Zaverucha for "An Attack on Some Signature Schemes Constructed From Five-Pass Identification Schemes"
- Andrea Caforio, Fatih Balli, and Subhadeep Banik for "Energy Analysis of Lightweight AEAD Circuits"
- Bar Meyuhas, Nethanel Gelernter, and Amir Herzberg for "Cross-Site Search Attacks: Unauthorized Queries over Private Data"

We were honored to have four keynote speakers: Atsuko Miyaji, Kenny Paterson, Mathias Payer, and Zhiyun Qian. We also had a tutorial by Amir Herzberg.

We would like to thank the ATHENE National Research Center for Applied Cybersecurity, as well as the H2020 initiative CyberSec4Europe, for their support during the planning of the conference. We would also like to thank Springer for their support with producing the proceedings. We heartily thank the authors of all submitted papers. Moreover, we are grateful to the members of the Program Committee and the external sub-reviewers for their diligent work, as well as all members of the Organizing Committee for their kind help. We would also like to acknowledge the Steering Committee for supporting us.

November 2020

Stephan Krenn
Haya Shulman
Serge Vaudenay

Organization

Steering Committee

Yvo G. Desmedt (Chair)	The University of Texas at Dallas, USA
Juan A. Garay	Texas A&M University, USA
Amir Herzberg	Bar-Ilan University, Israel
Yi Mu	Fujian Normal University, China
Panos Papadimitratos	KTH, Sweden
David Pointcheval	CNRS, ENS Paris, France
Huaxiong Wang	Nanyang Technological University, Singapore

PC Chairs

Haya Shulman	Fraunhofer SIT, Germany
Serge Vaudenay	Ecole Polytechnique Fédérale de Lausanne, Switzerland

General Chair

Stephan Krenn	AIT Austrian Institute of Technology, Austria

Organizing Committee

Manuela Kos	AIT Austrian Institute of Technology, Austria
Michael Mürling	AIT Austrian Institute of Technology, Austria
Krzysztof Pietrzak (Publicity Chair)	IST Austria, Austria
Hervais Simo	Fraunhofer SIT, Germany

Program Committee

Yehuda Afek	Tel-Aviv University, Israel
Steven Arzt	Fraunhofer, Germany
Xavier Boyen	Queensland University of Technology, Australia
Bremler Bremler-Barr	IDC, Israel
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong
Ran Cohen	Northeastern University, USA
Sabrina De Capitani di Vimercati	Universitá degli Studi di Milano, Italy
F. Betül Durak	Robert Bosch LLC, USA
Michael Franz	University of California, Irvine, USA
Flavio D. Garcia	University of Birmingham, UK

Peter Gaži	IOHK Research, Slovakia
Niv Gilboa	Ben-Gurion University, Israel
Dieter Gollmann	Hamburg University of Technology, Germany
Louis Goubin	Versailles Saint-Quentin-en-Yvelines University, France
Amir Herzberg	Department of Computer Science and Engineering, Israel
Sotiris Ioannidis	Technical University of Crete, Greece
Alptekin Küpçü	Koç University, Turkey
Atefeh Mashatan	Ryerson University, Canada
Kazuhiko Minematsu	NEC Corporation, Japan
Chris Mitchell	Royal Holloway, UK
Max Mühlhäuser	TU Darmstadt, Germany
Mridul Nandi	Indian Statistical Institute, India
Raphael C.-W. Phan	Monash University, Malaysia
Thomas Pornin	NCC Group, Canada
Neta Rozen-Schiff	Hebrew University of Jerulsalem, Israel
Mark Ryan	University of Birmingham, UK
Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Simona Samardjiska	Radboud University, The Netherlands
Gil Segev	Hebrew University of Jerusalem, Israel
Jean-Pierre Seifert	Technical University of Berlin, Germany
Haya Shulman	Fraunhofer, Germany
Cristian-Alexandru Staicu	CISPA Helmholtz Center for Information Security, Germany
Nikhil Tripathi	TU Darmstadt, Germany
Serge Vaudenay	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Damien Vergnaud	Sorbonne Université, Institut Universitaire de France, France
Ivan Visconti	Università degli Studi di Salerno, Italy
Damian Vizár	CSEM, Switzerland
Edgar Weippl	University of Vienna, Austria
Matthias Wählisch	Freie Universität Berlin, Germany
Avishay Yanai	VMware Research, Israel

External Reviewers

Abdulla Aldoseri	Augustin Bariant
Nikolaos Alexopoulos	Khashayar Barooti
Gennaro Avitabile	Andrea Basso
Shahar Azulay	Rishabh Bhadauria
Fatih Balli	Rishiraj Bhattacharyya
Subhadeep Banik	Osman Biçer

Leon Böck
Vincenzo Botta
Andrea Caforio
Fabio Campos
Avik Chakraborti
Gwangbae Choi
Daniel Collins
Sandro Coretti
Hila Dahari
Nilanjan Datta
Mohammad Sadeq Dousti
Cansu Dǒganay
Alexandre Duc
Sonia Duc
Minxin Du
Ehsan Ebrahimi
Rolf Egert
Keita Emura
Daniel Fentham
Georgios Fotiadis
Daniele Friolo
Sarah Gaballah
Reza Ghasemi
Anirban Ghatak
Simin Ghesmati
Satrajit Ghosh
Tim Grube
Mathias Gusenbauer
Ariel Hamlin
Yahya Hassanzadeh-Nazarabadi
Philipp Holzinger
Loïs Huguenin-Dumittan
Vincenzo Iovino
Novak Kaluderovic
Shankar Karuppayah
Handan Kılınç Alper
Maria Kober
Philip Kolvenbach
Veronika Kuchta
Mario Larangeira
Eysa Lee
Wanpeng Li
Fukang Liu
Jack P. K. Ma
Alexandra Mai
Lukas Malina
Karola Marky
Adrian Marotzke
Zdenek Martinasek
Soundes Marzougui
Marc Miltenberger
Jose Moreira
Johannes Mueller
Sayantan Mukherjee
Kit Murdock
Alon Noy (Neuhaus)
Lucien K. L. Ng
Mihai Ordean
Shinjo Park
Guillermo Pascual-Perez
Francesco Pasquale
Leo Perrin
Katharina Pfeffer
Niklas Pirnay
Andreea-Ina Radu
Eyal Ronen
Yann Rotella
Lior Rotem
Sujoy Sinha Roy
Pratik Sarkar
Liron Schiff
Philipp Schindler
Gili Schul-Ganz
Henning Seidler
Kris Shrishak
Rajiv Ranjan Singh
Marjan Skrobot
Najmeh Soroush
Aikaterini Sotiraki
Sanaz Taheri-Boshrooyeh
Hiroto Tamiya
Sam L. Thomas
Bénédikt Tran
Itay Tsabary
Andrea Tundis
Rei Ueno
Bogdan Ursu
Jeroen van Wier

Benoit Viguier
Aidmar Wainakh
Jiafan Wang
Thom Wiggers
Nils Wisiol
Donald P. H. Wong
Harry W. H. Wong
Zohar Yakhini
Hailun Yan
Yongjun Zhao

Contents