Lecture Notes in Computer Science 9696

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Mark Manulis · Ahmad-Reza Sadeghi
Steve Schneider (Eds.)

Applied Cryptography and Network Security

14th International Conference, ACNS 2016 Guildford, UK, June 19–22, 2016 Proceedings

Springer

Editors
Mark Manulis
Department of Computer Science
University of Surrey
Guildford
UK

Steve Schneider
Department of Computer Science
University of Surrey
Guildford
UK

Ahmad-Reza Sadeghi
CASED
Technische Universität Darmstadt
Darmstadt, Hessen
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-39554-8 ISBN 978-3-319-39555-5 (eBook)
DOI 10.1007/978-3-319-39555-5

Library of Congress Control Number: 2015958852

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

The 14th International Conference on Applied Cryptography and Network Security, ACNS 2016, took place June 19–22, 2016, in Guildford, UK, and was organized by the Surrey Centre for Cyber Security (SCCS) at the University of Surrey.

ACNS is an annual conference focusing on original research in applied cryptography, cyber security, and privacy. Both academic research with high relevance to real-world problems and developments in industrial and technical frontiers fall within the scope of the conference.

ACNS 2016 received 183 submissions, all of which were reviewed by the Program Committee. Each of the 49 Program Committee members was assigned an average of 11 submissions for review. Each paper was assigned to at least three reviewers, while submissions co-authored by Program Committee members were assigned to at least four reviewers. The Program Committee was helped by the reports and opinions of 138 external reviewers. The submission process was not anonymous and author names were visible to all reviewers. The review process was organized and managed through EasyChair. The reviewers were asked to declare any conflicts of interest for all submissions in the beginning of the process. The selection process was very competitive and after highly interactive discussions and a careful deliberation, 35 papers were selected by the Program Committee for presentation at the conference. This puts the acceptance rate of ACNS 2016 at 19 %.

The ACNS 2016 program included two invited talks: "Securing Positioning: From GPS to IoT" by Srdjan Capkun from ETH Zurich and "Foundations of Hardware-Based Attested Computation and Applications of SGX" by Bogdan Warinschi from Bristol University. The prize for the Best Student Paper was awarded to Elena Kirshanova and Friedrich Wiemer for their paper "Parallel Implementation of BDD Enumeration for LWE" co-authored with Alexander May.

ACNS 2016 was organized by Mark Manulis and Ahmad-Reza Sadeghi, who served as program chairs, selected the Program Committee, and led their efforts in choosing papers that you will find in this volume, and by Steve Schneider, who served as general chair and was helped in the local organization by Anna-Lisa Ferrara and Shujun Li.

The ACNS 2016 chairs would like to thank everyone who contributed to the success of the conference. We are grateful to the Program Committee and external reviewers for their commitment, hard work, and enthusiasm to ensure that each paper received a thorough and fair review. Last but not least, we wish to thank all conference participants for making ACNS 2016 an enjoyable experience.

June 2016

Mark Manulis
Ahmad-Reza Sadeghi
Steve Schneider

ACNS 2016

14th International Conference on Applied Cryptography and Network Security Guildford, UK, June 19–22, 2016

General Chair

Steve Schneider	University of Surrey, UK

Program Chairs

Mark Manulis	University of Surrey, UK
Ahmad-Reza Sadeghi	TU Darmstadt, Germany

Program Committee

Frederik Armknecht	University of Mannheim, Germany
Giuseppe Ateniese	Stevens Institute of Technology, USA
Elias Athanasopoulos	Vrije Universiteit Amsterdam, The Netherlands
Man Ho Au	Hong Kong Polytechnic University, China
Liqun Chen	Hewlett-Packard Laboratories, UK
Sherman S.M. Chow	Chinese University of Hong Kong, China
Mauro Conti	University of Padua, Italy
Lucas Davi	TU Darmstadt, Germany
Alexandra Dmitrienko	ETH Zurich, Switzerland
Michael Franz	University of California, Irvine, USA
Sebastian Gajek	NEC Laboratories Europe, Germany
Jens Groth	University College London, UK
Goichiro Hanaoka	AIST, Japan
Feng Hao	Newcastle University, UK
Michael Huth	Imperial College London, UK
Tibor Jager	Ruhr University Bochum, Germany
Yier Jin	University of Central Florida, USA
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Negar Kiyavash	University of Illinois, USA
Vladimir Kolesnikov	Bell Laboratories, USA
Mark Manulis	University of Surrey, UK
Ivan Martinovic	University of Oxford, UK

Azalia Mirhoseini	Rice University, USA
Atsuko Miyaji	JAIST, Japan
Payman Mohassel	University of Calgary, Canada
Jörn Müller-Quade	Karlsruhe Institute of Technology, Germany
David Naccache	Ecole Normale Superieure, France
Michael Naehrig	Microsoft Research Redmond, USA
Hamed Okhravi	MIT Lincoln Laboratory, USA
Claudio Orlandi	Aarhus University, Denmark
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden
Thomas Peyrin	Nanyang Technological University, Singapore
Bertram Poettering	Ruhr University Bochum, Germany
Bart Preneel	KU Leuven, Belgium
Jeyavijayan Rajendran	University of Texas at Dallas, USA
Christian Rechberger	Technical University of Denmark, Denmark
Peter Y. Ryan	University of Luxembourg, Luxembourg
Rei Safavi-Naini	University of Calgary, Canada
Thomas Schneider	TU Darmstadt, Germany
Ozgur Sinanoglu	NYU Abu Dhabi, UAE
Douglas Stebila	McMaster University, Canada
Thorsten Strufe	TU Dresden, Germany
Gang Tan	Penn State University, USA
Vanessa Teague	University of Melbourne, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Ivan Visconti	University of Salerno, Italy
Wenyuan Xu	University of South Carolina, USA
Moti Yung	Snapchat, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Dirk Achenbach
Sk Subidh Ali
Moreno Ambrosin
Kanishka Ariyapala
Afonso Arriaga
Tomer Ashur
Nuttapong Attrapadung
Saikrishna Badrinarayanan
David Barrera
Marc Beunardeau
David Bigelow
Begül Bilgin
Kaidel Bjoern
Jonathan Bootle
Joppe Bos
Colin Boyd
Ferdinand Brasser
Brandon Broadnax
Luigi Catuogno
Andrea Cerulli
Pyrros Chaidos
Sze Yiu Chau
Zhuo Chen
Michele Ciampi
Alberto Compagno
Heng Cui
Daniel Demmler
Alexander Detrano
Fraser Dickin
Christoph Dobraunig

Benjamin Dowling
Maria Eichelseder
Keita Emura
Hossein Fereidooni
Manuel Fersch
Houda Ferradi
Yuichi Futa
Rémi Géraud
Essam Ghadafi
Lorenzo Grassi
Stefano Guarino
Gus Gutoski
Britta Hale
Stephan Häuser
Matt Henricksen
Felix Heuer
Jialin Huang
Matthias Huber
Siam Hussain
Jean-Louis Huynen
Chandrakumar Holenarasipursuresh
Panagiotis Ilia
Vincenzo Iovino
Morshed Islam
Hakon Jacobsen
Angela Jäschke
Dirmanto Jap
Mahavir Jhawar
Sachhidh Kannan
Bhavana Kanukurthi
Arun Kanuparthi
Ghassan Karame
Pierre Karpman
Nikolaos Karvelas
Taechan Kim
Ágnes Kiss
Alexander Koch
Stefan Koelbl
Matthias Krause
Russell W.F. Lai
Kim Laine
Chhagan Lal
Charles Lamech
Sebastian Lauer
Hoon Wei Lim
Shen Liu
Xiruo Liu
Patrick Longa
Jiqiang Lu
Stefan Lucks
Daniel Masny
Takahiro Matsuda
Bodhisatwa Mazumdar
Florian Mendel
Alfred Menezes
Vasily Mikhalev
Vladislav Mladlenov
Paweł Morawiecki
Pedro Moreno-Sanchez
Matthias Nagel
Ivica Nikolic
Go Ohtake
Kazumasa Omote
Cristina Onete
Jiaxin Pan
Panagiotis Papadopoulos
Arpita Patra
Umberto Ferraro Petrillo
Antigoni Polychroniadou
Ivan Pryvalov
Kim Ramchen
Sadegh Riazi
Peter B. Roenne
Stefanie Roos
Arnab Roy
Sujoy Sinha Roy
Bita Rouhani
Vladimir Rozic
Tim Ruffing
Yusuke Sakai
Hani Salah
Jacob Schuldt
Alexander Senier
Hwajeong Seo
Setareh Sharifian
Siang Meng Sim
Luisa Siniscalchi
Juraj Somorovsky
Ebrahim Songhori
Riccardo Spolaor
Richard Skowyra
Marjan Skrobot

Chunhua Su
Somayeh Taheri
Katsuyuki Takashima
Qiang Tang
Tyge Tiessen
Elmar Tischhauser
Thao Tran
Pengwei Wang
Qingju Wang
Xiuhua Wang
Xueyang Wang
Marcel Winandy
Miao Xu
Jia Xu
Shota Yamada
Rupeng Yang
Muhammad Yasin
Shaza Zeitouni
Dongrui Zeng
Liang Feng Zhang
Tao Zhang
Zongyang Zhang
Yongjun Zhao
Luying Zhou
Michael Zohner

Contents

DoS Attacks and Network Anomaly Detection

Deterministic and Functional Encryption

Computing on Encrypted Data

Non-Interactive Proofs and PRFs

Symmetric Ciphers

Cryptography in Software

Security for Human Use