Lecture Notes in Computer Science 7954

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

Michael Jacobson Michael Locasto
Payman Mohassel Reihaneh Safavi-Naini (Eds.)

Applied Cryptography and Network Security

11th International Conference, ACNS 2013
Banff, AB, Canada, June 25-28, 2013
Proceedings

Springer

Volume Editors

Michael Jacobson
Michael Locasto
Payman Mohassel
Reihaneh Safavi-Naini

University of Calgary, Department of Computer Science
2500 University Drive NW, Calgary, AB T2N 1N4, Canada

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-38979-5 e-ISBN 978-3-642-38980-1
DOI 10.1007/978-3-642-38980-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013940302

CR Subject Classification (1998): K.6.5, E.3, K.4.4, D.4.6, E.4, C.2, J.1, E.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

ACNS 2013, the 11th International Conference on Applied Cryptography and Network Security, was held during June 25–28 at Banff, Alberta, Canada.

We received 150 submissions of which 33 were accepted as regular papers (22% acceptance rate), and two as short papers. These proceedings contain the revised versions of all the papers. There were three invited talks. Srdjan Capkun, Professor of Computer Science at ETH Zurich, gave a talk entitled "Selected Topics in Wireless Physical Layer Security." Bryan Parno from Microsoft Research Redmond, gave a talk on "Bootstrapping Cloud Security Speaker," and Francois Theberge, research mathematician with the Tutte Institute for Mathematics and Computing spoke about "Ensemble Clustering for Graphs-Based Data."

The Program Committee (PC) consisted of 35 members with diverse research interest and experience. Papers were reviewed double-blind, with each paper assigned to three reviewers. During the discussion phase, when necessary, extra reviews were solicited. We ensured that all papers received fair and objective evaluation by experts and also a broader group of PC members, with particular attention paid to highlighting strengths and weaknesses of papers. The final decisions were made based on the reviews and discussion. The task of paper selection was especially challenging given the high number of strong submissions. In the end, a sizable number of strong papers could not be included in the program owing to lack of space.

We would like to sincerely thank authors of all submissions– those whose papers made it into the program and those whose papers did not. We, and the PC as a whole, were impressed by the quality of submissions contributed from all around the world. Although this made the task of selecting the final list very challenging, it gave us the opportunity to have a strong and diverse program.

We would like to extend our sincere gratitude to the Program Committee. We were very fortunate that so many talented people put such an inordinate amount of time to write reviews and actively participate in discussions for nearly three weeks. They responded to our requests for extra reviews, opinions, comments, comparisons, and inputs. We were impressed by the knowledge, dedication, and integrity of our PC. We also would like to thank many external reviewers, some contacted by us directly and some through PC members, who significantly contributed to the comprehensive evaluation of papers. A list of PC members and external reviewers appears after this note.

We would like to thank Mahabir Jhanwar, the Publicity Chair, for working closely with us throughout the whole process, providing the much needed support in every step. We would also like to thank Tongjie Zhang for handling our social media presence, Coral Burns for her work on the ACNS website, Deb Angus for logistical and administrative support, Camille Sinanan for her help with the local organization and financial administration, and, finally, Hadi Ahmadi and

numerous student volunteers who helped us with the successful organization of the program.

We benefited from advice and feedback from Moti Yung and Jianying Zhou, the ACNS Steering Committee. Alfred Hofmann and his colleagues at Springer provided a meticulous service for the timely production of this volume.

We would like to thank Microsoft Research, the Pacific Institute for Mathematical Sciences (PIMS), Alberta Innovates Technology Future (AITF), and the University of Calgary for their generous support. We also gratefully acknowledge our partnership with the Tutte Institute for Mathematics and Computing (TIMC), in contributing to the success of this conference.

April 2013

Michael Jacobson
Michael Locasto
Payman Mohassel
Reihaneh Safavi-Naini

ACNS 2013

11th International Conference on Applied Cryptography and Network Security

BANFF, Alberta, Canada June 25–28, 2013

General Chairs

Michael Jacobson	University of Calgary, Canada
Payman Mohassel	University of Calgary, Canada

Program Chairs

Michael Locasto	University of Calgary, Canada
Reihaneh Safavi-Naini	University of Calgary, Canada

Program Committee

Bill Aiello	University of British Columbia, Canada
Giuseppe Ateniese	Sapienza University of Rome, Italy
Kevin R.B. Butler	University of Oregon, USA
Srdjan Capkun	ETH Zurich, Switzerland
Alvaro A. Cárdenas	University of Texas at Dallas, USA
Chen-Mou Cheng	National Taiwan University, Taiwan
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong
Ed Dawson	Queensland University of Technology, Australia
Roberto Di Pietro	Università Roma Tre, Italy
Sara Foresti	Università degli Studi di Milano, Italy
Guang Gong	University of Waterloo, Canada
Stefanos Gritzalis	University of the Aegean, Greece
Guofei Gu	Texas A&M University, USA
Angelos D. Keromytis	Columbia University, USA
Evangelos Kranakis	Carleton University, Canada
Ralf Küsters	Universität Trier, Germany
Xuejia Lai	Shanghai Jiao Tong University, China
Cédric Lauradoux	INRIA, France
Ninghui Li	Purdue University, USA
Yingjiu Li	Singapore Management University, Singapore
Mark Manulis	University of Surrey, UK
Kaisa Nyberg	Aalto University, Finland
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	DTU, Denmark

Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Radu Sion	Stony Brook University, USA
Anil Somayaji	Carleton University, Canada
Abhinav Srivastava	AT&T Research, USA
Jessica Staddon	Google, USA
Willy Susilo	University of Wollongong, Australia
Gene Tsudik	UC Irvine, USA
Duncan S. Wong	City University of Hong Kong, Hong Kong
Jianying Zhou	I^2R, Singapore

Publicity Chair

Mahabir P. Jhanwar	University of Calgary, Canada

Steering Committee

Yongfei Han	ONETS, China
Moti Yung	Google, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Additional Reviewers

Achara, Jagdish	Chia, Pern	Huang, Jialin
Ahmadi, Hadi	Choi, Seung Geol	Huang, Qiong
Albrecht, Martin R.	Chu, Cheng-Kang	Huang, Xinyi
Alimomeni, Mohsen	Cunche, Mathieu	Huang, Zhengan
Andreeva, Elena	Damopoulos, Dimitrios	Huo, Fei
Androulaki, Elli	De Cristofaro, Emiliano	Jhanwar, Mahabir
Argyros, George	Ding, Jintai	Jiang, Shaoquan
Armknecht, Frederik	Dmitrienko, Alexandra	Kalloniatis, Christos
Athanasopoulos, Elias	Fan, Junfeng	Kambourakis, Georgios
Au, Man Ho	Fan, Xinxin	Kemerlis, Vasileios P.
Bae, Jun-Young	Fang, Liming	Kerschbaum, Florian
Baig, Basim	Fett, Daniel	Kim, Jihye
Bajaj, Sumeet	Fleischhacker, Nils	Konidala, Divyan
Balopoulos, Theodoros	Gagne, Martin	Kontaxis, Georgios
Bernstein, Daniel J.	Gajek, Sebastian	Krell, Fernando
Bloch, Mathieu	Geneiatakis, Dimitris	Krenn, Stephan
Blondeau, Céline	Gervais, Arthur	Kuo, Po-Chun
Boggs, Nathaniel	Ghodosi, Hossein	Lafourcade, Pascal
Boura, Christina	Gong, Zheng	Lange, Tanja
Boyd, Colin	Gorantla, Choudary	Lauridsen, Martin M.
Boyen, Xavier	Groth, Jens	Li, Ming
Cao, Jianneng	Guarino, Stefano	Li, Yan
Chandran, Nishant	Guo, Fuchun	Liang, Kaitai
Chang, Yun-An	Han, Jin	Liu, Joseph

Liu, Zhen
Lombardi, Flavio
Long, Yu
Ma, Di
Malisa, Luka
Mandal, Kalikinkar
Miettinen, Markus
Mohassel, Payman
More, Sara
Mouha, Nicky
Nergiz, Ahmet Erhan
Nguyen, Lan
Niederhagen, Ruben
Nikolic, Ivica
Nikova, Svetla
Nishide, Takashi
Núñez, David
Olejnik, Lukasz
Pappas, Vasilis
Peeters, Roel
Peikert, Chris
Pointcheval, David
Polychronakis, Michalis
Popper, Christina
Radomirovic, Sasa
Ranganathan, Aanjhan
Rasmussen, Kasper Bonne
Rial, Alfredo
Rizomiliotis, Panagiotis
Rouselakis, Yannis
Salim, Farzad
Schmitz, Guido
Schneider, Michael
Sepehrdad, Pouyan
Shahandashti, Siamak
Soleimany, Hadi
Soriente, Claudio
Su, Dong
Tan, Xiao
Tuengerthal, Max
Tzouramanis, Theodoros
Ustaoglu, Berkant
Vahlis, Yevgeniy
Van Herrewege, Anthony
Varici, Kerem
Villani, Antonio
Vo, Binh
Vogt, Andreas
Wachsmann, Christian
Wu, Jong-Shian
Wu, Teng
Xie, Xiang
Xu, Hong
Xu, Jia
Xu, Zhaoyan
Xue, Weijia
Yang, Chao
Yang, Guomin
Yang, Yanjiang
Yu, Ching-Hua
Yuen, Tsz Hon
Zhang, Cong
Zhang, Haibin
Zhang, Jialong
Zhang, Liangfeng
Zhang, Tao
Zhou, Xuhua
Zhu, Bo

Table of Contents

Cloud Cryptography

Secure Computation

Hash Function and Block Cipher

Signature

Group-Oriented Cryptography

System Attack I

Secure Implementation – Hardware

Secure Implementation – Software

System Attack II

Group-Oriented Systems

Key Exchange and Leakage Resilience

Cryptographic Proof

Cryptosystems