Lecture Notes in Computer Science 6123

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

Jianying Zhou Moti Yung (Eds.)

Applied Cryptography and Network Security

8th International Conference, ACNS 2010
Beijing, China, June 22-25, 2010
Proceedings

Springer

Volume Editors

Jianying Zhou
Institute for Infocomm Research
1 Fusionopolis Way, Singapore, 138632, Singapore
E-mail: jyzhou@i2r.a-star.edu.sg

Moti Yung
Google Inc. and Columbia University
Computer Science Department
New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2010928335

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-13707-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13707-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

ACNS 2010, the 8th International Conference on Applied Cryptography and Network Security, was held in Beijing, China, during June 22-25, 2010. ACNS 2010 brought together individuals from academia and industry involved in multiple research disciplines of cryptography and security to foster the exchange of ideas.

ACNS was initiated in 2003, and there has been a steady improvement in the quality of its program over the past 8 years: ACNS 2003 (Kunming, China), ACNS 2004 (Yellow Mountain, China), ACNS 2005 (New York, USA), ACNS 2006 (Singapore), ACNS 2007 (Zhuhai, China), ACNS 2008 (New York, USA), ACNS 2009 (Paris, France). The average acceptance rate has been kept at around 17%, and the average number of participants has been kept at around 100.

The conference received a total of 178 submissions from all over the world. Each submission was assigned to at least three committee members. Submissions co-authored by members of the Program Committee were assigned to at least four committee members. Due to the large number of high-quality submissions, the review process was challenging and we are deeply grateful to the committee members and the external reviewers for their outstanding work. After extensive discussions, the Program Committee selected 32 submissions for presentation in the academic track, and these are the articles that are included in this volume (LNCS 6123). Additionally, a few other submissions were selected for presentation in the non-archival industrial track. The prize for the best student paper was awarded to Mehdi Tibouchi for his paper "On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption", co-authored with Aurelie Bauer, Jean-Sebastien Coron, David Naccache, and Damien Vergnaud.

We would like to thank General Chair Yongfei Han and the local organizing team from Beijing University of Technology and ONETS for their efforts in putting this conference together. Our special thanks are due to Ying Qiu for managing the Easy Chair system for paper submission and review. We would also like to thank all the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

April 2010

Jianying Zhou
Moti Yung

ACNS 2010

8th International Conference on
Applied Cryptography and Network Security

Beijing, China
June 22–25, 2010

Organized and Sponsored by

Beijing University of Technology & ONETS, China

General Chair

Yongfei Han	BJUT & ONETS, China

Program Chairs

Jianying Zhou	Institute for Infocomm Research, Singapore
Moti Yung	Columbia University & Google, USA

Program Committee

Michel Abdalla	ENS, France
Ben Adida	Harvard University, USA
N. Asokan	Nokia, Finland
Joonsang Baek	I2R, Singapore
Lucas Ballard	Google, USA
Feng Bao	I2R, Singapore
Lujo Bauer	Carnegie Mellon University, USA
Alex Biryukov	Uni. of Luxembourg, Luxembourg
Alexandra Boldyreva	Georgia Tech, USA
Colin Boyd	QUT, Australia
Levente Buttyan	BME, Hungary
Liqun Chen	HP Laboratories, UK
Songqing Chen	George Mason University, USA
Debra Cook	Telcordia, USA
Cas Cremers	ETH Zurich, Switzerland
Sabrina De Capitani di Vimercati	UNIMI, Italy
Robert Deng	SMU, Singapore

Orr Dunkelman	Weizmann Institute, Israel
Dieter Gollmann	TU Hamburg-Harburg, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Marc Joye	Technicolor, France
Charanjit Jutla	IBM, USA
Angelos Keromytis	Columbia University, USA
Xuejia Lai	Shanghai Jiao Tong University, China
Dong Hoon Lee	Korea University, Korea
Ninghui Li	Purdue University, USA
Yingjiu Li	SMU, Singapore
Benoit Libert	UCL, Belgium
Dongdai Lin	Institute of Software, China
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Mark Manulis	TU Darmstadt, Germany
Fabio Martinelli	CNR, Italy
Atefeh Mashatan	EPFL, Switzerland
Paolo Milani	Technical University of Vienna, Austria
Chris Mitchell	RHUL, UK
Atsuko Miyaji	JAIST, Japan
Tatsuaki Okamoto	NTT, Japan
Alina Oprea	RSA Laboratories, USA
Elisabeth Oswald	University of Bristol, UK
Benny Pinkas	University of Haifa, Israel
Pandu Rangan	Indian Institute of Technology, India
Vincent Rijmen	TU Graz, Austria
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	Ruhr-Uni. Bochum, Germany
Reihaneh Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Nitesh Saxena	Poly Institute of New York Uni., USA
Radu Sion	Stony Brook University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	FUN, Japan
Duncan Wong	City University of Hong Kong, China

Organizing Chairs

Jian Li	Beijing University of Technology, China
Yu Wang	ONETS, China

Publicity Chairs

Javier Lopez	University of Malaga, Spain
Tsuyoshi Takagi	FUN, Japan
Sijin Li	ONETS, China

Steering Committee

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

External Reviewers

Gergely Acs
Isaac Agudo
Efthimia Aivaloglou
Mansoor Alicherry
Elli Androulaki
Myrto Arapinis
Frederik Armknecht
Tomoyuki Asano
Elias Athanasopoulos
Man Ho Au
Jean-Philippe Aumasson
Sumeet Bajaj
Collard Baudoin
Bruno Blanchet
Marina Blanton
Shaoying Cai
Tianjie Cao
Bogdan Carbunar
Julien Cathalo
Sambuddho Chakravarty
Shiping Chen
Wei Cheng
Kyu Young Choi
Tom Chothia
Cheng-Kang Chu
Ji Young Chun
Gabriele Costa
Gabriela Cretu
Ning Ding
Alexandra Dmitrienko
Ming Duan
Mark Felegyhazi
Carmen Fernandez-Gago
Dario Fiore
Martin Gagne
Zheng Gong
Juan Gonzalez
Choudary Gorantla
Tzipora Halevi
Christoph Herbst
Shlomo Hershkop
Tamas Holczer
Qiong Huang
Toshiyuki Isshiki
Stas Jarecki
Ayman Jarrous
Seny Kamara
Giorgos Karopoulos
Vasileios P. Kemerlis
Bum Han Kim
Kitak Kim
Ilya Kizhvatov
Miroslav Knezevic
Clemens Kolbitsch
Deguang Kong
Elisavet Konstantinou
Woo Kwon Koo
Leanid Krautsevich
Swarun Kumar
Virendra Kumar
Francesco la Torre
Fabien Laguillaumie
Aliaksandr Lazouski
Hyun Sook Lee
Kwangsu Lee
Fagen Li
Tieyan Li
Wei Li
Yan Li
Jingqiang Lin
Hanwu Liu
Joseph. K. Liu
Mei Cheng Liu
Xianhui Lu
Christoph Ludwig
Yiyuan Luo
Hans Lohr
Ilaria Matteucci
Marcel Medwed
Daisuke Moriyama
Andreas Moser
Francisco Moyano
Pablo Najera
Toru Nakanishi
Kris Narayan
Kris Narayan
Matthias Neugschwandtner
Ching Yu Ng
Ivica Nikolic
Geon Tae Noh
Adam O'Neill
Wakaha Ogata
Katsuyuki Okeya
Kazumasa Omote
Khaled Ouafi
Carles Padro
Jung Ha Paik
Vasilis Pappas
Sai Tej Peddinti
Chris Peikert
Kun Peng
Christophe Petit
Thomas Plantard
Bertram Poettering
Mariana Raykova
Tzachy Reinman
Evangelos Reklitis
Ruben Rios
Panagiotis Rizomiliotis
Rodrigo Roman

Bagus Santoso
Werner Schindler
Michael Schneider
Thomas Schneider
Dominique Schroder
Sharmila Deva selvi
Nicolas Sendrier
Daniele Sgandurra
Siamak Shahandashti
Jun Shao
Takeshi Shimoyama
Francesco Sica
Stelios Sidiroglou
Matt Smart
Nigel Smart
Ben Smyth
Miroslava Sotakova
Douglas Stebila
Thorsten Strufe
Chunhua Su
Xiaorui Sun
Martin Szydlowski
Kouya Tochikubo
Ashraful Tuhin
Michael Tunstall
Berkant Ustaoglu
Istvan Vajda
Serge Vaudenay
Jose Luis Vivas
Sree Vivek
Jonathan Voris
Camille Vuillaume
Christian Wachsmann
Zhongmei Wan
Xinyuan Wang
Ralf-Philipp Weinmann
Zhongming Wu
Fubiao Xia
Jing Xu
Guanhua Yan
Qiang Yan
Guomin Yang
Artsiom Yautsiukhin
Kuo-Hui Yeh
Kazuki Yoneyama
Junfeng Yu
Tsz Hon Yuen
Angelika Zavou
Bin Zhang
Min Zhang
Mingwu Zhang
Shengzhi Zhang
Xinwen Zhang
Yunlei Zhao
JinMin Zhong
Chunfang Zhou
Hong-Sheng Zhou
Bo Zhu

Table of Contents

Public Key Encryption

Digital Signature

Block Ciphers and Hash Functions

Side-Channel Attacks

Zero Knowledge and Multi-party Protocols

Key Management

Authentication and Identification

Privacy and Anonymity

RFID Security and Privacy

Internet Security