Lecture Notes in Computer Science 5339

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

Matthew K. Franklin Lucas Chi Kwong Hui
Duncan S. Wong (Eds.)

Cryptology and Network Security

7th International Conference, CANS 2008
Hong-Kong, China, December 2-4, 2008
Proceedings

Springer

Volume Editors

Matthew K. Franklin
University of California
Department of Computer Science
Davis, CA, USA
E-mail: franklin@cs.ucdavis.edu

Lucas Chi Kwong Hui
The University of Hong Kong
Department of Computer Science
Hong Kong, China
E-mail: hui@cs.hku.hk

Duncan S. Wong
City University of Hong Kong
Department of Computer Science
Hong Kong, China
E-mail: duncan@cityu.edu.hk

Library of Congress Control Number: 2008939862

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-89640-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-89640-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12577507 06/3180 5 4 3 2 1 0

Preface

The seventh international conference on Cryptology and Network Security (CANS 2008) was held at HKU Town Center, Hong Kong, China, during December 2–4, 2008. The conference was organized by the Department of Computer Science, the University of Hong Kong, and was fully supported by the Center for Information Security and Cryptography at the University of Hong Kong, the Cyberport Institute of Hong Kong at the University of Hong Kong and the Department of Computer Science at the City University of Hong Kong.

The goal of CANS is to promote research on all aspects of network security, as well as to build a bridge between research on cryptography and network security. Previous CANS conferences have been held in Taipei, Taiwan (2001), San Francisco, USA (2002), Miami, USA (2003), Xiamen, China (2005), Suzhou, China (2006), and Singapore (2007). The conference proceedings of recent years were published by Springer in the *Lecture Notes in Computer Science* series.

The Program Committee received 73 submissions, and accepted 27 papers for presentation. The final versions of the accepted papers, which the authors finalized on the basis of comments from the reviewers, were included in the proceedings. The reviewing process took nine weeks; each paper was carefully evaluated by at least three members from the Program Committee. The individual reviewing phase was followed by a Web-based discussion. Based on the comments and scores given by reviewers, the final decisions on acceptance were made. We appreciate the hard work of the members of the Program Committee and the external referees who gave many hours of their valuable time.

In addition to the contributed papers, there were two invited talks. One was given by Juan Garay and the other one was by Xiaoyun Wang.

We would like to thank all the people involved in organizing this conference. In particular, we would like to thank the Organizing Committee members, colleagues and our student helpers for their time and effort. Finally, we would like to thank all the authors who submitted papers to the conference.

December 2008

Matthew K. Franklin
Lucas Chi Kwong Hui
Duncan S. Wong

Organization

CANS 2008 was organized by the Department of Computer Science, The University of Hong Kong, China, and held during December 2–4, 2008.

General Chair

Lucas C.K. Hui	The University of Hong Kong, China

Program Co-chairs

Matt Franklin	UC Davis, USA
Duncan S. Wong	City University of Hong Kong, China

Steering Committee

Yvo Desmedt	University College London, UK
Matt Franklin	UC Davis, USA
Yi Mu	University of Wollongong, Australia
David Pointcheval	CNRS and ENS, France
Huaxiong Wang	Nanyang Technological University, Singapore

Organizing Committee

K.P. Chow	The University of Hong Kong, China
Bruce Cheung	The University of Hong Kong, China
Lucas C.K. Hui	The University of Hong Kong, China
Raymond Szeto	The University of Hong Kong, China

Program Committee

Michel Abdalla	École Normale Supérieure, France
Joonsang Baek	I2R, Singapore
Feng Bao	I2R, Singapore
Hao Chen	East China Normal University, China
Liqun Chen	HP Bristol Labs, UK
Mike Burmester	Florida State University, USA
Ed Dawson	QUT, Australia
Robert Deng	SMU, Singapore
Dengguo Feng	Chinese Academy of Sciences, China
Eiichiro Fujisaki	NTT Labs, Japan

Jun Furukawa	NEC, Japan
David Galindo	University of Malaga, Spain
Aline Gouget	Gemalto, France
Aggelos Kiayias	University of Connecticut, USA
Eike Kiltz	CWI, The Netherlands
Kwangjo Kim	Info. and Comm. University, Korea
Dong Hoon Lee	Korea University, Korea
Arjen Lenstra	EPFL, Switzerland
Benoit Libert	UCL, Belgium
Javier Lopez	University of Malaga, Spain
Mitsuru Matsui	Mitsubishi Electric, Japan
Yi Mu	University of Wollongong, Australia
Jörn Müller-Quade	Universität Karlsruhe, Germany
Tatsuaki Okamoto	NTT Labs, Japan
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
C. Pandu Rangan	IIT, India
Berry Schoenmakers	TU Eindhoven, The Netherlands
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Guilin Wang	University of Birmingham, UK
Huaxiong Wang	NTU, Singapore
Xiaoyun Wang	Tsinghua/Shandong University, China
Yiqun Lisa Yin	Independent Consultant, USA
Fangguo Zhang	Sun Yat-sen University, China
Yunlei Zhao	Fudan University, China
Jianying Zhou	I2R, Singapore

External Reviewers

Man Ho Au	Flavio Garcia	Paul Morrissey
Shaoying Cai	Qiong Huang	Kyosuke Osaka
David Cash	Xinyi Huang	Arpita Patra
Julien Cathalo	Vincenzo Iovino	Wen-Feng Qi
Kyu Young Choi	Bum Han Kim	Yi Qian
Ashish Choudary	Jangseong Kim	Chun Ruan
Ji Young Chun	Daniel Kraschewski	German Saez
Andrew Clark	Hwaseong Lee	Jason Smith
Blandine Debraize	Ji-Seon Lee	Xiao Tan
Cécile Delerablée	Jiguo Li	Ivan Visconti
Nico Döttling	Jin Li	Sree Vivek
Sharmila devi selvi	Tieyan Li	Baodian Wei
Oriol Farras	Xibin Lin	Jian Weng
Clemente Galdi	Jospeh K. Liu	Wei Wu
Debin Gao	George Mohay	Xiaokang Xiong

Guomin Yang
Yanjiang Yang
Chan Yeob Yeun
Jeong Jae Yu
Yong Yu
Tsz Hon Yuen
Yao-Dong Zhao

Supporting Institutions

Center for Information Security and Cryptography (CISC), The University of Hong Kong, China
The Cyberport Institute of Hong Kong, The University of Hong Kong, China
Department of Computer Science, City University of Hong Kong, China

Table of Contents

Cryptosystems

Signatures

Identification, Authentication and Key Management

Cryptographic Algorithms and Protocols

Stream Ciphers and Block Ciphers

Cryptographic Foundations

Applications and Implementations

Security in Ad Hoc Networks and Wireless Sensor Networks