Lecture Notes in Computer Science 5222

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

Tzong-Chen Wu Chin-Laung Lei
Vincent Rijmen Der-Tsai Lee (Eds.)

Information Security

11th International Conference, ISC 2008
Taipei, Taiwan, September 15-18, 2008
Proceedings

Springer

Volume Editors

Tzong-Chen Wu
National Taiwan University of Science and Technology
Department of Information Management
No. 43, Sec. 4, Keelung Road, Taipei 106, Taiwan
E-mail: tcwu@cs.ntust.edu.tw

Chin-Laung Lei
National Taiwan University, Department of Electrical Engineering
No. 1, Sec. 4, Roosevelt Road, Taipei 106, Taiwan
E-mail: lei@cc.ee.ntu.edu.tw

Vincent Rijmen
Graz University of Technology
Institute for Applied Information Processing and Communications (Austria)
Katholieke Universiteit Leuven, Department of Electrical Engineering (Belgium)
Inffeldgasse 16a, 8010 Graz, Austria
E-mail: Vincent.Rijmen@iaik.tugraz.at

Der-Tsai Lee
Academia Sinica, Institute of Information Science
No. 128, Sec. 2, Academia Road, Nankang, Taipei 115, Taiwan
E-mail: dtlee@iis.sinica.edu.tw

Library of Congress Control Number: 2008933846

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-85884-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85884-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12517565 06/3180 5 4 3 2 1 0

Preface

The 11th Information Security Conference (ISC 2008) was held in Taipei, Taiwan, September 15–18, 2008. ISC is an annual international conference covering research in theory and applications of information security. It was first initiated as a workshop (ISW) in Japan in 1997. This was followed by ISW 1999 in Malaysia and ISW 2000 in Australia. ISW became ISC when it was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), UK (ISC 2003), USA (ISC 2004), Singapore (ISC 2005), Greece (ISC 2006), and Chile (ISC 2007). This year the event was sponsored by the Chinese Cryptology and Information Security Association (Taiwan), the Taiwan Information Security Center of the Research Center for IT Innovation (Academia Sinica, Taiwan), the National Taiwan University of Science and Technology (Taiwan), the NTU Center for Information and Electronics Technologies (Taiwan), Academia Sinica (Taiwan), the National Science Council (Taiwan), the Ministry of Education (Taiwan), the Taipei Chapter of the IEEE Computer Society (Taiwan), BankPro E-service Technology Co., Ltd. (Taiwan), Exsior Data & Information Technology, Inc. (Taiwan), Giga-Byte Education Foundation (Taiwan), Hewlett-Packard Taiwan, Hivocal Technologies, Co., Ltd. (Taiwan), Microsoft Taiwan, Paysecure Technology Co., Ltd. (Taiwan), Symlink (Taiwan), and Yahoo! Taiwan Holdings Limited (Taiwan Branch).

In order to cover the conference's broad scope, this year's main Program Committee consisted of 61 experts from 22 countries. Additionally, the conference also featured a special AES Subcommittee, chaired by Vincent Rijmen (Graz University of Technology, Austria).

The conference received 134 submissions from 31 countries, 33 (including 4 in the AES special session) of which were selected by the committee members for presentation at the conference, based on quality, originality and relevance. Each paper was anonymously reviewed by at least three committee members. In order to encourage and promote student participation, the ISC 2008 Program Committee selected three student-coauthored papers for the Best Student Paper award, one from each region: Asia, Europe, and the Americas. The papers were, respectively, "Deterministic Constructions of 21-Step Collisions for the SHA-2 Hash Family," by Somitra Sanadhya and Palash Sarkar (Indian Statistical Institute, India), "Collisions for RC4-Hash," by Sebastiaan Indesteege and Bart Preneel (Katholieke Universiteit Leuven, Belgium), and "Proxy Re-signatures in the Standard Model," by Sherman S.M. Chow (New York University, USA) and Raphael Phan (Loughborough University, UK). The program also included invited speeches by Doug Tygar (UC Berkeley, USA) and Tatsuaki Okamoto (NTT, Japan).

Many people helped to make ISC 2008 successful. We would like to thank all those who contributed to the technical program and to organizing the conference. We are very grateful to the Program Committee members and the external referees for their efforts in reviewing and selecting the papers. We would like to express our

special thanks to all the organizing committee members for making the conference possible. We also give our thanks to all the authors of the submitted papers and the invited speakers for their contributions to the conference.

July 2008

Tzong-Chen Wu
Chin-Laung Lei

ISC 2008

The 11th International Security Conference
Taipei, Taiwan, September 15–18, 2008

General Chair

Der-Tsai Lee	Director of the Institute of Information Science, Academia Sinica, Taiwan

Steering Committee

Ed Dawson	Queensland University of Technology, Australia
Der-Tsai Lee	Academia Sinica, Taiwan
Javier López	University of Málaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Eiji Okamoto	University of Tsukuba, Japan
René Peralta	NIST, USA
Rebecca Wright	Rutgers University, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

Program Co-chairs

Tzong-Chen Wu	National Taiwan University of Science and Technology, Taiwan
Chin-Laung Lei	National Taiwan University, Taiwan

Finance Chairs

Jason Shih	Paysecure Technology Co., Ltd., Taiwan
Tim Chiou	Microsoft Corporation
David Fan	Exsior Data & Information Technology, Inc., Taiwan

Publications Chairs

D.J. Guan	National Sun Yat-Sen University, Taiwan
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Chun-I Fan	National Sun Yat-Sen University, Taiwan

Local Arrangements Chairs

Hahn-Ming Lee	National Taiwan University of Science and Technology, Taiwan
Ren-Junn Hwang	Tamkang University, Taiwan
Ming-Hour Yang	Chung Yuan Christian University, Taiwan

Registration Chairs

Wei-Hua He	Soochow University, Taiwan
Shiuh-Jeng Wang	National Central Police University, Taiwan
Wen-Shenq Juang	National Kaohsiung First University of Science and Technology, Taiwan

Publicity Chairs

Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Hung-Min Sun	National Tsing Hua University, Taiwan
Chien-Lung Hsu	Chang Gung University, Taiwan

Web Masters

Bo-Yin Yang	Institute of Information Science, Academia Sinica, Taiwan
Chun-Yang Chen	Institute of Information Science, Academia Sinica, Taiwan
Chen-Mou Cheng	National Taiwan University, Taiwan

Program Committee

Mikhail Atallah	Purdue University, USA
Feng Bao	Institute for Infocomm Research, Singapore
David Basin	ETH Zurich, Switzerland
Josh Benaloh	Microsoft Research, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Johannes Buchmann	TU Darmstadt, Germany
David Chadwick	University of Kent, UK
Tsuhan Chen	Carnegie Mellon University, USA
Tzi-Cker Chiueh	State University of New York at Stony Brook, USA
Debbie Cook	Bell Labs, USA
Robert Deng	Singapore Management University, Singapore
Xiaotie Deng	City University of Hong Kong, China
Claudia Diaz	Katholieke Universiteit Leuven, Belgium
Jintai Ding	University of Cincinnati, USA
Chun-I. Fan	National Sun Yat-Sen University, Taiwan
Pierre-Alain Fouque	ENS, France
Juan Garay	Bell Labs, USA
Shai Halevi	IBM Research, USA
Wei-Hua He	Soochow University, Taiwan
Amir Herzberg	Bar-Ilan University, Israel

Dennis Hofheinz	CWI, Netherlands
Lei Hu	State Key Laboratory of Information Security, China
Ren-Junn Hwang	Tamkang University, Taiwan
Marc Joye	Thomson R&D, France
Wen-Shenq Juang	National Kaohsiung First University of Science and Technology, Taiwan
Hiroaki Kikuchi	Tokai University, Japan
Kwangjo Kim	Information and Communication University, Korea
Seungjoo Kim	Sungkyunkwan University, Korea
Marcos Kiwi	University of Chile, Chile
Spyros Kokolakis	University of the Aegean, Greece
Steve Kremer	ENS Cachan, France
Xuejia Lai	Shanghai Jiao Tong University, China
Ruby Lee	Princeton University, USA
San Ling	Nanyang Technological University, Singapore
Subhamoy Maitra	Indian Statistical Institute, India
Keith Martin	RH University of London, UK
Fabio Massacci	University of Trento, Italy
Breno de Medeiros	Google, USA
Chris Mitchell	RH University of London, UK
Atsuko Miyaji	JAIST, Japan
Fabian Monrose	Johns Hopkins University, USA
Hikaru Morita	Kanagawa University, Japan
David Naccache	Gemplus, France
Koji Nakao	KDDI, Japan
Kaisa Nyberg	Helsinki University of Technology and Nokia, Finland
Carles Padró	Polytechnic University of Catalonia, Spain
Adrian Perrig	Carnegie Mellon University, USA
Andreas Pfitzmann	Dresden University of Technology , Germany
Raphael Phan	Loughborough University, UK
Josef Pieprzyk	Macquarie University, Australia
Rei Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Angelos Stavrou	George Mason University, USA
Dominique Unruh	Saarland University, Germany
Ariel Waissbein	ITBA and Core Security, Argentina
Felix Wu	UC Davis, USA
Huaxiong Wang	Nanyang Technological University, Singapore
Bo-Yin Yang	Academia Sinica, Taiwan
Kan Yasuda	NTT, Japan
Heung Youl Youm	Soonchunhyang University/IITA, Korea

AES Subcommittee

Joan Daemen	STMicroelectronics Belgium, Belgium
Xuejia Lai	Shanghai Jiao Tong University, China
Chi Sung Laih	National Cheng Kung University, Taiwan
Vincent Rijmen	Graz University of Technology, Austria
Matt Robshaw	France Telecom, France
Hung-Min Sun	National Tsing Hua University, Taiwan
Ralph Wernsdorf	Rohde & Schwarz, Germany

External Reviewers

Guido Bertoni	Stijn Lievens
Rainer Böhme	Chu-Hsing Lin
Elie Bursztein	Hubert Comon-Lundh
Kostas Chatzikokolakis	Serdar Pehlivanoglu
Jung-Hui Chiu	Duong Hieu Phan
Kim-Kwang Raymond Choo	Natalya Rassadko
Sherman S.M. Chow	Ermaliza Razali
Ricardo Corin	Ayda Saidane
Oriol Farras	Stefan Schiffner
Hani Hassen	Sandra Steinbrecher
Matt Henricksen	Ruggero Susella
Alejandro Hevia	Carmela Troncoso
Vladimir Kolesnikov	Guilin Wang
Gabriel Kuper	Shiuh-Jeng Wang
Cedric Lauradoux	Artsiom Yautsiukhin
Jia-Hong Lee	Sung-Ming Yen

Sponsoring Institutions

Chinese Cryptology and Information Security Association (CCISA), Taiwan
Taiwan Information Security Center (TWISC), Center for IT Innovation, Academia Sinica, Taiwan
National Taiwan University of Science and Technology (NTUST), Taiwan
NTU Center for Information and Electronics Technologies (NTU CIET), Taiwan
Academia Sinica, Taiwan
National Science Council (NSC), Taiwan
Ministry of Education, Taiwan
IEEE Computer Society, Taipei Chapter
BankPro E-service Technology Co., Ltd. (Taiwan)
Exsior Data & Information Technology, Inc. (Taiwan)

Giga-Byte Education Foundation (Taiwan)
Hivocal Technologies, Co., Ltd. (Taiwan)
Microsoft Taiwan
Paysecure Technology Co., Ltd. (Taiwan)
Symlink (Taiwan)
Yahoo! Taiwan Holdings Limited (Taiwan Branch)

Table of Contents

Trusted Computing

Database and System Security

Intrusion Detection

Network Security

Cryptanalysis

Digital Signatures

AES Special Session

Symmetric Cryptography and Hash Functions

Authentication

Security Protocols