Lecture Notes in Computer Science 4861

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

Editorial Board

Sihan Qing Hideki Imai Guilin Wang (Eds.)

Information and Communications Security

9th International Conference, ICICS 2007
Zhengzhou, China, December 12-15, 2007
Proceedings

Springer

Volume Editors

Sihan Qing
Chinese Academy of Sciences
Institute of Software
Beijing 100080, China
E-mail: qsihan@ss.pku.edu.cn

Hideki Imai
Chuo University
Faculty of Science and Engineering
Tokyo 112-8551, Japan
E-mail: h-imai@aist.go.jp

Guilin Wang
University of Birmingham
School of Computer Science
Birmingham B15 2TT, UK
E-mail: G.Wang@cs.bham.ac.uk

Library of Congress Control Number: 2007940029

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77047-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77047-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12198054 06/3180 5 4 3 2 1 0

Preface

The ninth International Conference on Information and Communications Security, ICICS 2007, was held in Zhengzhou, Henan Province, China, December 12–15, 2007. The ICICS conference series is an established forum that brings together people working in different fields of information and communications security from universities, research institutes, industry and government institutions, and gives the attendees the opportunity to exchange new ideas and investigate state-of-the-art developments. Among the preceding conferences, ICICS 1997 took place in Beijing, China; ICICS 1999 in Sydney, Australia; ICICS 2001 in Xi'an, China; ICICS 2002 in Singapore; ICICS 2003 in Huhehaote city, China; ICICS 2004 in Malaga, Spain; ICICS 2005 in Beijing, China; and ICICS 2006 in Raleigh, NC, USA. The proceedings were released as Volumes 1334, 1726, 2229, 2513, 2836, 3269, 3783, and 4307 of the Springer LNCS series, respectively.

ICICS 2007 was sponsored by the Chinese Academy of Sciences (CAS), the Beijing Natural Science Foundation of China under Grant No. 4052016 and the National Natural Science Foundation of China under Grant No. 60573042. The conference was organized and hosted by the Institute of Software, Chinese Academy of Sciences, Institute of Software and Microelectronics, Peking University, and ZhongAn Scientific and Technological Group in co-operation with the Informatization Office of Provincial Government of Henan, China and the International Communications and Information Security Association (ICISA).

In total, 222 papers from 19 countries and districts were submitted to ICICS 2007, and 38 were accepted covering multiple disciplines of information security and applied cryptography. From those papers accepted, 13 were from China, five from USA, four from Australia, three from Singapore, two each from Hong Kong, Iran, Japan and Taiwan, and one each from Belgium, Canada, Germany, Korea, and UK.

All submissions to ICICS 2007 were anonymously reviewed by at least two PC members, while the majority were commented on by three or more reviewers. The reviewing process took six weeks. We are grateful to the Program Committee, which was composed of 56 members from 19 countries and districts; we thank them as well as all external referees for their precious time and valued contributions to the tough and time-consuming reviewing process.

We thank Guilin Wang for his great work in arranging the publishing of the proceedings, Jiayong Cai for his great contribution to the pre-conference arrangements, and Dadong Li, Jianbo He, Qi Guo and others from the Organizing Committee for helping with many local details.

Finally, we would like to thank all the authors who submitted their papers to ICICS 2007, and all the attendees from all over the world.

October 2007

Sihan Qing
Hideki Imai

ICICS 2007

Ninth International Conference
on Information and Communications Security

Zhengzhou, Henan Province, China
December 12–15, 2007

Organized by

ZhongAn Scientific and Technological Group, China
Institute of Software, Chinese Academy of Sciences (CAS)
Institute of Software and Microelectronics, Peking University, China

In co-operation with

Informatization Office of Provincial Government of Henan, China
International Communications and Information Security Association (ICISA)

Sponsored by

Chinese Academy of Sciences (CAS)
Beijing Natural Science Foundation of China
National Natural Science Foundation of China (NNSFC)

General Chair

Sihan Qing	Chinese Academy of Sciences, China

Program Chairs

Sihan Qing	Chinese Academy of Sciences, China
Hideki Imai	University of Tokyo, Japan

Program Committee

Mikhail Atallah	Purdue University, USA
Vijay Atluri	Rutgers University, USA
Tuomas Aura	Microsoft, UK
Michael Backes	Saarland University, Germany
Thomas Berson	Anagram Laboratories, USA
Elisa Bertino	Purdue University, USA

Alex Biryukov	University of Luxembourg, Luxembourg
Srdjan Capkun	ETH Zurich, Switzerland
Chin-Chen Chang	Feng Chia University, Taiwan
Hao Chen	University of California at Davis, USA
Zhong Chen	Peking University, China
Stelvio Cimato	University of Milan, Italy
Bruno Crispo	Vrije University, The Netherlands
Edward Dawson	Queensland University of Technology, Australia
Robert H. Deng	Singapore Management University, Singapore
David Evans	University of Virginia, USA
David Grawrock	Intel, USA
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Yong Guan	Iowa State University, USA
James Heather	University of Surrey, UK
Kwanjo Kim	Information and Communications University, Korea
Engin Kirda	Technical University of Vienna, Austria
Paris Kitsos	Hellenic Open University, Greece
Chi-Sung Laih	National Cheng Kung University, Taiwan
Ninghui Li	Purdue University, USA
Yingjiu Li	Singapore Management University, Singapore
Jong-in Lim	Korea University, Korea
Javier Lopez	University of Malaga, Spain
Wenbo Mao	EMC, USA
Chris Mitchell	Royal Holloway, UK
Peng Ning	North Carolina State University, USA
Eiji Okamoto	University of Tsukuba, Japan
Giuseppe Persiano	Università di Salerno, Italy
Raphael C.-W. Phan	EPFL, Switzerland
Radha Poovendran	University of Washington, USA
Jean-Jacques Quisquater	UCL Crypto Group, Belgium
Kai Rannenberg	Goethe University Frankfurt, Germany
Indrajit Ray	University of Birmingham, UK
Bimal Roy	Indian Statistical Institute, India
Mark Ryan	University of Birmingham, UK
Kouichi Sakurai	Kyushu University, Japan
Ryoichi Sasaki	Tokyo Denki University, Japan
Miguel Soriano	Technical University of Catalonia, Spain
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Wade Trappe	Rutgers University, USA
Guilin Wang	I^2R, Singapore and University of Birmingham, UK
Andreas Wespi	IBM Zurich, Switzerland
Duncan S. Wong	City University of Hong Kong, China

S. Felix Wu	University of California at Davis, USA
Yongdong Wu	Institute for Infocomm Research, Singapore
Alec Yasinsac	Florida State University, USA
Lisa Yiqun Yin	Independent Security Consultant, USA
Moti Yung	Columbia University & RSA Labs, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Pennsylvania State University, USA

Publication Chair

Guilin Wang	I^2R, Singapore and University of Birmingham, UK

Organizing Committee Chair

Dadong Li	Zhongan Technology Group Co., Ltd., China

External Reviewers

Andreas Albers	Man Ho Au	Jean-Philippe Aumasson
Joonsang Baek	Matthias Berg	Abhilasha Bhargav-Spantzel
Colin Boyd	Chiara Braghin	Sherman S.M. Chow
Cas Cremers	Marco Cremonini	S. Delaune
Yi Deng	André Deuker	Jintai Ding
Anh Dinh	Oscar Esparza	Chun-I Fan
Gerardo Fernandez	Carmen Fernandez-Gago	Annalisa Ferrara
Ernest Foo	Lothar Fritsch	Liang Gu
Keisuke Hakuta	Matt Henricksen	Juan Hernández-Serrano
Yoshiaki Hori	Lei Hu	Qiong Huang
Xinyi Huang	Kitae Jeong	Qingguang Ji
Jianchun Jiang	Haimin Jin	Audun Josang
Jorge Nakahara Jr	Christian Kahl	Ashish Kamra
Khoongming Khoo	Jongsung Kim	Tae Hyun Kim
Steve Kremer	Jin Kwak	Fagen Li
Tieyan Li	Zhuowei Li	Phen-Lan Lin
Joseph K. Liu	Liang Low	Luke McAven
Shiho Moriai	Aybek Mukhamedov	José L. Muñoz-Tapia
Toru Nakanishi	Juan Gonzalez Nieto	Stanley R. de Medeiros Oliveira
Josep Pegueroles	Kun Peng	Hasan Qunoo
Havard Raddum	Mike Radmacher	Sanjay Rawat
Rodrigo Roman	Denis Royer	Eve Schooler
Chang Shuang	Leonie Simpson	Chunhua Su
Christophe Tartary	Hayo Thielecke	Duc Liem Vo
Falk Wagner	Zhiguo Wan	Chih-Hung Wang

Chuen-Ching Wang
Peng Wang
Qihua Wang
Shuhong Wang
Ralf-Philipp Weinmann
Zhe Xia
Guomin Yang
Yanjiang Yang
Wentao Zhang
Zhengfeng Zhang
Yunlei Zhao
Yongbin Zhou
Bo Zhu
Jan Zibuschka

Table of Contents

Authentication and Key Exchange

Digital Signatures

Applications

Watermarking

Fast Implementations

Applied Cryptography

Cryptanalysis

Formal Analysis

System Security I

System Security II

Network Security