Lecture Notes in Computer Science 5927

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

Sihan Qing Chris J. Mitchell
Guilin Wang (Eds.)

Information and Communications Security

11th International Conference, ICICS 2009
Beijing, China, December 14-17, 2009
Proceedings

Springer

Volume Editors

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

Chris J. Mitchell
University of London, Information Security Group
Egham, Surrey TW20 0EX, United Kingdom
E-mail: c.mitchell@rhul.ac.uk

Guilin Wang
University of Birmingham, School of Computer Science
Birmingham, B15 2TT, United Kingdom
E-mail: g.wang@cs.bham.ac.uk

Library of Congress Control Number: 2009940402

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-11144-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-11144-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12809325 06/3180 5 4 3 2 1 0

Preface

The 11th International Conference on Information and Communications Security (ICICS 2009) was held in Beijing, China during December 14–17, 2009. The ICICS conference series is an established forum that brings together people from universities, research institutes, industry and government institutions, who work in a range of fields within information and communications security. The ICICS conferences give attendees the opportunity to exchange new ideas and investigate developments in the state of the art. In previous years, ICICS has taken place in the UK (2008), China (2007, 2005, 2003, 2001 and 1997), USA (2006), Spain (2004), Singapore (2002), and Australia (1999). On each occasion, as on this one, the proceedings have been published in the Springer LNCS series.

In total, 162 manuscripts from 20 countries and districts were submitted to ICICS 2009, and a total of 37 (31 regular papers plus 6 short papers) from 13 countries and districts were accepted (an acceptance rate of 23%). The accepted papers cover a wide range of disciplines within information security and applied cryptography. Each submission to ICICS 2009 was anonymously reviewed by three or four reviewers. We are very grateful to members of the Program Committee, which was composed of 44 members from 14 countries; we would like to thank them, as well as all the external referees, for their time and their valuable contributions to the tough and time-consuming reviewing process.

In addition to the contributed speakers, the program also featured two invited speakers in the technical track. We are grateful to Richard A. Kemmerer (University of California, Santa Barbara, USA), and Wenbo Mao (EMC, USA), for accepting our invitation to speak. We also thank the keynote speakers from TCG on the first day of the conference, which was devoted to the industrial aspects of trusted and trustworthy computing.

ICICS 2009 was organized and hosted by the Institute of Software, Chinese Academy of Sciences (CAS), and the Institute of Software and Microelectronics, Peking University in co-operation with International Communications and Information Security Association (ICISA). The conference was sponsored by the National Natural Science Foundation of China under Grant No. 60573042 and No. 60970135, the Microsoft Corporation, Beijing Tip Technology Corporation, and the Trusted Computing Group (TCG).

We would like to thank Guilin Wang for his great work in arranging the publishing of the proceedings, and Dongmei Liu for her great contribution to the pre-conference arrangements and helping with many local details. Finally, we would like to thank the authors who submitted their papers to ICICS 2009, and the attendees from all around the world.

October 2009

Sihan Qing
Chris J. Mitchell

ICICS 2009

11th International Conference
on Information and Communications Security

Beijing, China
December 14–17, 2009

Organized by

Institute of Software, Chinese Academy of Sciences (CAS)
Institute of Software and Microelectronics, Peking University, China

Sponsored by

National Natural Science Foundation of China (NNSFC)
The Microsoft Corporation
Beijing Tip Technology Corporation, China
Trusted Computing Group (TCG)

In co-operation with

International Communications and Information Security Association (ICISA)

General Chair

Fuqing Yang	Peking University, China

Vice Chair

Zhong Chen	Peking University, China

Program Chairs

Sihan Qing	Chinese Academy of Sciences and Peking University, China
Chris J. Mitchell	Royal Holloway, University of London, UK

Program Committee

Mikhail Atallah	Purdue University, USA
Tuomas Aura	Microsoft Research, UK
Thomas Berson	Anagram Laboratories, USA
Alex Biryukov	University of Luxembourg, Luxembourg

Srdjan Capkun	ETH Zurich, Switzerland
Chin-Chen Chang	Feng Chia University, Taiwan
Liqun Chen	Hewlett-Packard Laboratories, Bristol, UK
Zhong Chen	Peking University, China
Bruno Crispo	University of Trento, Italy
Edward Dawson	Queensland University of Technology, Australia
Dengguo Feng	Chinese Academy of Sciences, China
Yong Guan	Iowa State University, USA
Yeping He	Chinese Academy of Sciences, China
James Heather	University of Surrey, UK
Chi-Sung Laih	National Cheng Kung University, Taiwan
Gaicheng Li	Peking University, China
Yingjiu Li	Singapore Management University, Singapore
Javier Lopez	University of Malaga, Spain
Wenbo Mao	EMC Research, China
Peng Ning	North Carolina State University, USA
Xinxin Niu	Beijing University of Posts and Telecommunications, China
Eiji Okamoto	University of Tsukuba, Japan
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
Qingni Shen	Peking University, China
Miguel Soriano	Technical University of Catalonia, Spain
Jinshu Su	National University of Defense Technology, China
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Guilin Wang	University of Birmingham, UK
Weiping Wen	Peking University, China
Andreas Wespi	IBM Zurich Research Laboratory, Switzerland
Duncan S. Wong	City University of Hong Kong, China
Wenling Wu	Chinese Academy of Sciences, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Yixian Yang	Beijing University of Posts and Telecommunications, China
Alec Yasinsac	Florida State University, USA
Wentao Zhang	Chinese Academy of Sciences, China
Jianying Zhou	Institute for Infocomm Research, Singapore
Qiming Zhou	Chinese Academy of Sciences, China

Publication Chair

Guilin Wang	University of Birmingham, UK

Organizing Committee

Qing Yu	Beijing Tip Technology Corporation, China (Chair)
Dongmei Liu	Chinese Academy of Sciences, China
Qiming Zhou	Chinese Academy of Sciences, China
Qingni Shen	Peking University, China
Weiping Wen	Peking University, China
Gaicheng Li	Peking University, China

External Reviewers

Man Ho Au
Ahmed Azab
Goekhan Bal
Bruno Blanchet
Jijun Cao
Pei-Te Chen
Qingkui Chen
Xiaofeng Chen
Cheng-Kang Chu
Mauro Conti
Boris Danev
Oscar Esparza
Xiutao Feng
Lothar Fritsch
Ge Fu
D. J. Guan
Juan Hernández-Serrano
Thomas S. Heydt-Benjamin
Xinyi Huang
Qingguang Ji
Chunfu Jia
Jianchun Jiang
Ghassan Karame
Wen-Chung Kuo
Stewart Kowalski
Fagen Li
Qiming Li
Rongsheng Li
Chuanglou Lin
Huan-Ping Liu
Joseph K. Liu
Stephan Neuhaus
Ivica Nikolic
Federica Paci
Thomas Plantard
Christina Poepper
Mike Radmacher
Kasper Rasmussen
Chun Ruan
Steve Schneider
Masaaki Shirase
Mario Strasser
Nils Tippenhauer
Joan Tomàs-Buliart
Markus Tschersich
Falk Wagner
Licheng Wang
Shaobing Wang
Shengyuan Wang
Xiaofeng Wang
Christian Weber
Ralf-Philipp Weinmann
Wei Wu
Zhe Xia
Jing Xu
Ziyao Xu
Yanjiang Yang
Ziye Yang
Attila Altay Yavuz
Davide Zanetti
Yingzhi Zeng
Bin Zhang
Fengli Zhang
Jingcheng Zhang
Mingwu Zhang
Baokang Zhao
Wen Tao Zhu

Table of Contents

Security Applications

Software Security

System Security

Network Security

Short Papers I

Database Security

Trust Management

Applied Cryptography

Short Papers II