Lecture Notes in Computer Science 5308

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

Liqun Chen Mark D. Ryan Guilin Wang (Eds.)

Information and Communications Security

10th International Conference, ICICS 2008
Birmingham, UK, October 20 - 22, 2008
Proceedings

Springer

Volume Editors

Liqun Chen
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol BS34 8QZ, UK
E-mail: liqun.chen@hp.com

Mark D. Ryan
Guilin Wang
University of Birmingham
School of Computer Science
Edgbaston, Birmingham B15 2TT, UK
E-mail: {m.d.ryan, g.wang}@cs.bham.ac.uk

Library of Congress Control Number: 2008936716

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-88624-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-88624-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12539420 06/3180 5 4 3 2 1 0

Preface

The 10th International Conference on Information and Communications Security (ICICS) was held in Birmingham, UK, during 20–22 October 2008. 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. In previous years, ICICS has taken place in China (2007, 2005, 2003, 2001, 1997), USA (2006), Spain (2004), Singapore (2002), and Australia (1999). On each occasion, as on this one, the proceedings were published in the Springer LNCS series.

In total, 125 papers from 33 countries were submitted to ICICS 2008, and 27 were accepted covering multiple disciplines of information security and applied cryptography (acceptance rate 22%). Each submission to ICICS 2008 was anonymously reviewed by three or four reviewers. We are grateful to the Programme Committee, which was composed of 57 members from 12 countries; we thank them as well as all external referees for their time and valued contributions to the tough and time-consuming reviewing process.

In addition to the contributed speakers, the programme also featured three invited speakers. We are grateful to Joshua Guttman (The MITRE Corporation, USA), Peng Ning (North Carolina State University, USA), and Nigel Smart (University of Bristol, UK) for accepting our invitation to speak.

ICICS 2008 was organised by the University of Birmingham and Hewlett Packard Laboratories. We gratefully acknowledge sponsorship from the UK Engineering and Physical Sciences Research Council (EPSRC), as well as Hewlett Packard and the University of Birmingham.

Organising a conference is difficult and time-consuming work. We are very grateful to Andy Brown, who worked tirelessly in making arrangements with the Hyatt Hotel and with the University of Birmingham, as well as maintaining the conference website. Also thanks to Ben Smyth for making a great job of collecting the papers together for these proceedings. Thanks also to Hasan Qunoo for helping with many local details. Finally, we would like to thank all the authors who submitted their papers to ICICS 2008, and all the attendees from all over the world.

October 2008

Liqun Chen
Mark Ryan
Guilin Wang

Organisation

ICICS 2008

10th International Conference on Information and Communications Security

Birmingham, UK October 20–22, 2008

Organised by

School of Computer Science, University of Birmingham, UK

Sponsored by

Engineering and Physical Sciences Research Council (EPSRC)
Hewlett-Packard Laboratories
University of Birmingham

In co-operation with

International Communications and Information Security Association (ICISA)

General Chair

Mark Ryan	University of Birmingham, UK

Programme Chairs

Liqun Chen	Hewlett-Packard Laboratories, UK
Mark Ryan	University of Birmingham, UK
Guilin Wang	University of Birmingham, UK

Programme Committee

Mikhail Atallah	Purdue University, USA
Tuomas Aura	Microsoft Research, UK
Vijay Atluri	Rutgers University, USA
Michael Backes	Saarland University, Germany
Feng Bao	Institute for Infocomm Research, Singapore
Elisa Bertino	Purdue University, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Colin Boyd	Queensland University of Technology, Australia
Srdjan Capkun	ETH Zurich, Switzerland

Chin-Chen Chang	Feng Chia University, Taiwan
Hao Chen	University of California at Davis, USA
Kefei Chen	Shanghai Jiaotong University, China
Edward Dawson	Queensland University of Technology, Australia
Robert Deng	Singapore Management University, Singapore
Dengguo Feng	Chinese Academy of Science, China
Steve Furnell	University of Plymouth, UK
Dieter Gollmann	Hamburg University of Technology, Germany
David Grawrock	Intel, USA
Hongxia Jin	IBM Almaden Research Center, USA
Engin Kirda	Institute Eurecom, France
Steve Kremer	ENS de Cachan, France
Chi-Sung Laih	National Cheng Kung University, Taiwan
Dong Hoon Lee	Korea University, Korea
Ninghui Li	Purdue University, USA
Qun Li	College of William and Mary, USA
Yingjiu Li	Singapore Management University, Singapore
Javier Lopez	University of Malaga, Spain
Wenbo Mao	EMC Research, China
Catherine Meadows	Naval Research Laboratory, USA
Chris Mitchell	Royal Holloway, UK
Sang-Jae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
Peng Ning	North Carolina State University, USA
Eiji Okamoto	University of Tsukuba, Japan
Akira Otsuka	AIST, Japan
Kenneth Paterson	Royal Holloway, UK
Giuseppe Persiano	Università di Salerno, Italy
Raphael Phan	Loughborough University, UK
Sihan Qing	Chinese Academy of Sciences, China
Kui Ren	Illinois Institute of Technology, USA
Eike Ritter	University of Birmingham, UK
Bimal Roy	Indian Statistical Institute, India
Peter Ryan	University of Newcastle, UK
Kouichi Sakurai	Kyushu University, Japan
Steve Schneider	University of Surrey, UK
Wenchang Shi	Renmin University of China, China
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Bogdan Warinschi	Universtiy of Bristol, UK
Andreas Wespi	IBM Zurich Research Laboratory, Switzerland
Duncan S. Wong	City University of Hong Kong, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Alec Yasinsac	Florida State University, USA
Moti Yung	Columbia University, USA

Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Penn State University, USA

Organising Committee

Andrew Brown	University of Birmingham, UK
Hasan Qunoo	University of Birmingham, UK
Ben Smyth	University of Birmingham, UK
Guilin Wang	University of Birmingham, UK

Publication Chairs

Ben Smyth	University of Birmingham, UK
Guilin Wang	University of Birmingham, UK

External Reviewers

Isaac Agudo
Cristina Alcaraz
Man Ho Au
Jean-Philippe Aumasson
Vicente Benjumea
Shaoying Cai
Giacomo Cancelli
Jianhong Chen
Carlos Cid
Andrew Clark
Nathan Clarke
Yvonne Cliff
Xuhua Ding
Rong Du
Markus Duermuth
Marie Duflot
Serge Fehr
Marcel Fernandez
Carmen Fernandez-Gago
Ernest Foo
Clemente Galdi
Juan Gonzalez
Jae-Cheol Ha
Manabu Hagiwara
Keisuke Hakuta
Hao Han
Wei Han
Keith Harrison
Nick Hoare
Xuan Hong
Yoshiaki Hori
Cătălin Hriţcu
Qiong Huang
Xinyi Huang
Jung Yeon Hwang
Manabu Inuma
Yoon-Chan Jhi
Qingguang Ji
Ashish Kamra
Takashi Kitagawa
Shinsaku Kiyomoto
Ilya Kizhvatov
Boris Köpf
Ji-Seon Lee
Fagen Li
Gaicheng Li
Jun Li
Bing Liang
Huo-Chong Ling
Joseph Liu
Yu Long
JiQiang Lu
Di Ma
Wenbo Mao
Miodrag Mihaljevic
George Mohay
Ian Molloy
Shiho Moriai
Qun Ni
Chihiro Ohyama
Elisabeth Oswald
Maria Papadaki
Jong Hwan Park
Serdar Pehlivanoglu
Jason Reid
Mohammad-Reza Reyhanitabar
Bo Sheng
Nicholas Sheppard
SeongHan Shin
Taizo Shirai
Leonie Simpson
Hui Song
Graham Steel
Makoto Sugita
Ashwin Swaminathan
Chiu Tan
Hitoshi Tanuma

Alberto Trombetta
Ivan Visconti
Yongtao Wang
Xinran Wang
Haodong Wang
Qihua Wang
Gaven Watson
Jian Weng
Zhe Xia
Liang Xie
Fengyuan Xu
Guomin Yang
Yanjiang Yang
Ng Ching Yu
Rui Zhang
Jinmin Zhong
Jakub Zimmermann

Table of Contents

Invited Talk

Authentication

Side Channel Analysis

Cryptanalysis

Access Control

Software Security

System Security

Applied Cryptography

Security Protocols