

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

Information and Communications Security

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

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

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

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

Table of Contents

Invited Talk

Attestation: Evidence and Trust	1
<i>George Coker, Joshua Guttman, Peter Loscocco, Justin Sheehy, and Brian Sniffen</i>	

Authentication

A Novel Solution for End-to-End Integrity Protection in Signed PGP Mail.....	19
<i>Lijun Liao and Jörg Schwenk</i>	
Unclonable Lightweight Authentication Scheme	33
<i>Ghaith Hammouri, Erdinç Öztürk, Berk Birand, and Berk Sunar</i>	
Threat Modelling in User Performed Authentication	49
<i>Xun Dong, John A. Clark, and Jeremy L. Jacob</i>	
Access with Fast Batch Verifiable Anonymous Credentials.....	65
<i>Ke Zeng</i>	

Side Channel Analysis

Quantifying Timing Leaks and Cost Optimisation	81
<i>Alessandra Di Pierro, Chris Hankin, and Herbert Wiklicky</i>	
Method for Detecting Vulnerability to Doubling Attacks	97
<i>Chong Hee Kim and Jean-Jacques Quisquater</i>	
Side Channel Analysis of Some Hash Based MACs: A Response to SHA-3 Requirements	111
<i>Praveen Gauravaram and Katsuyuki Okeya</i>	

Cryptanalysis

Key Recovery Attack on Stream Cipher Mir-1 Using a Key-Dependent S-Box	128
<i>Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, and Tomoyasu Suzaki</i>	
Analysis of Two Attacks on Reduced-Round Versions of the SMS4	141
<i>Deniz Toz and Orr Dunkelman</i>	

Applying Time-Memory-Data Trade-Off to Meet-in-the-Middle Attack	157
<i>Jiali Choy, Khoongming Khoo, and Chuan-Wen Loe</i>	

Access Control

Beyond User-to-User Access Control for Online Social Networks	174
<i>Mohamed Shehab, Anna Cinzia Squicciarini, and Gail-Joon Ahn</i>	
Revocation Schemes for Delegation Licences	190
<i>Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia, and Adel Bouhoula</i>	
Reusability of Functionality-Based Application Confinement Policy Abstractions	206
<i>Z. Cliffe Schreuders and Christian Payne</i>	
Towards Role Based Trust Management without Distributed Searching of Credentials	222
<i>Gang Yin, Huaimin Wang, Jianquan Ouyang, Ning Zhou, and Dianxi Shi</i>	

Software Security

BinHunt: Automatically Finding Semantic Differences in Binary Programs	238
<i>Debin Gao, Michael K. Reiter, and Dawn Song</i>	
Enhancing Java ME Security Support with Resource Usage Monitoring	256
<i>Alessandro Castrucci, Fabio Martinelli, Paolo Mori, and Francesco Roperti</i>	
Pseudo-randomness Inside Web Browsers	267
<i>Zhi Guan, Long Zhang, Zhong Chen, and Xianghao Nan</i>	

System Security

Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data	279
<i>Henrich C. Pöhls</i>	
Embedding Renewable Cryptographic Keys into Continuous Noisy Data	294
<i>Ileana Buhan, Jeroen Doumen, Pieter Hartel, Qiang Tang, and Raymond Veldhuis</i>	

Automated Device Pairing for Asymmetric Pairing Scenarios	311
<i>Nitesh Saxena and Md. Borhan Uddin</i>	

Applied Cryptography

Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0.	328
<i>Nicolas T. Courtois and Blandine Debraize</i>	
Towards an Information Theoretic Analysis of Searchable Encryption . . .	345
<i>Saeed Sedghi, Jeroen Doumen, Pieter Hartel, and Willem Jonker</i>	
A Bootstrap Attack on Digital Watermarks in the Frequency Domain	361
<i>Sam Behseta, Charles Lam, and Robert L. Webb</i>	
Improved Data Hiding Technique for Shares in Extended Visual Secret Sharing Schemes	376
<i>Rabia Sirhindi, Saeed Murtaza, and Mehreen Afzal</i>	

Security Protocols

Efficient Multi-authorizer Accredited Symmetrically Private Information Retrieval	387
<i>Mohamed Layouni, Maki Yoshida, and Shingo Okamura</i>	
Specification of Electronic Voting Protocol Properties Using ADM Logic: FOO Case Study	403
<i>Mehdi Talbi, Benjamin Morin, Valérie Viet Triem Tong, Adel Bouhoula, and Mohamed Mejri</i>	
Publicly Verifiable Remote Data Integrity	419
<i>Ke Zeng</i>	
Author Index	435