Information and Communications Security

10th International Conference, ICICS 2008
Birmingham, UK, October 20 - 22, 2008
Proceedings
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
<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chin-Chen Chang</td>
<td>Fengchia University, Taiwan</td>
</tr>
<tr>
<td>Hao Chen</td>
<td>University of California at Davis, USA</td>
</tr>
<tr>
<td>Kefei Chen</td>
<td>Shanghai Jiaotong University, China</td>
</tr>
<tr>
<td>Edward Dawson</td>
<td>Queensland University of Technology, Australia</td>
</tr>
<tr>
<td>Robert Deng</td>
<td>Singapore Management University, Singapore</td>
</tr>
<tr>
<td>Dengguo Feng</td>
<td>Chinese Academy of Science, China</td>
</tr>
<tr>
<td>Steve Furnell</td>
<td>University of Plymouth, UK</td>
</tr>
<tr>
<td>Dieter Gollmann</td>
<td>Hamburg University of Technology, Germany</td>
</tr>
<tr>
<td>David Grawrock</td>
<td>Intel, USA</td>
</tr>
<tr>
<td>Hongxia Jin</td>
<td>IBM Almaden Research Center, USA</td>
</tr>
<tr>
<td>Engin Kirda</td>
<td>Institute Eurecom, France</td>
</tr>
<tr>
<td>Steve Kremer</td>
<td>ENS de Cachan, France</td>
</tr>
<tr>
<td>Chi-Sung Laih</td>
<td>National Cheng Kung University, Taiwan</td>
</tr>
<tr>
<td>Dong Hoon Lai</td>
<td>Korea University, Korea</td>
</tr>
<tr>
<td>Ninghui Li</td>
<td>Purdue University, USA</td>
</tr>
<tr>
<td>Qun Li</td>
<td>College of William and Mary, USA</td>
</tr>
<tr>
<td>Yingjiu Li</td>
<td>Singapore Management University, Singapore</td>
</tr>
<tr>
<td>Javier Lopez</td>
<td>University of Malaga, Spain</td>
</tr>
<tr>
<td>Wenbo Mao</td>
<td>EMC Research, China</td>
</tr>
<tr>
<td>Catherine Meadows</td>
<td>Naval Research Laboratory, USA</td>
</tr>
<tr>
<td>Chris Mitchell</td>
<td>Royal Holloway, UK</td>
</tr>
<tr>
<td>Sang-Jae Moon</td>
<td>Kyungpook National University, Korea</td>
</tr>
<tr>
<td>Yi Mu</td>
<td>University of Wollongong, Australia</td>
</tr>
<tr>
<td>Peng Ning</td>
<td>North Carolina State University, USA</td>
</tr>
<tr>
<td>Eiji Okamoto</td>
<td>University of Tsukuba, Japan</td>
</tr>
<tr>
<td>Akira Otsuka</td>
<td>AIST, Japan</td>
</tr>
<tr>
<td>Kenneth Paterson</td>
<td>Royal Holloway, UK</td>
</tr>
<tr>
<td>Giuseppe Persiano</td>
<td>Università di Salerno, Italy</td>
</tr>
<tr>
<td>Raphael Phan</td>
<td>Loughborough University, UK</td>
</tr>
<tr>
<td>Sihan Qing</td>
<td>Chinese Academy of Sciences, China</td>
</tr>
<tr>
<td>Kui Ren</td>
<td>Illinois Institute of Technology, USA</td>
</tr>
<tr>
<td>Eike Ritter</td>
<td>University of Birmingham, UK</td>
</tr>
<tr>
<td>Bimal Roy</td>
<td>Indian Statistical Institute, India</td>
</tr>
<tr>
<td>Peter Ryan</td>
<td>University of Newcastle, UK</td>
</tr>
<tr>
<td>Kouichi Sakurai</td>
<td>Kyushu University, Japan</td>
</tr>
<tr>
<td>Steve Schneider</td>
<td>University of Surrey, UK</td>
</tr>
<tr>
<td>Wenchang Shi</td>
<td>Renmin University of China, China</td>
</tr>
<tr>
<td>Willy Susilo</td>
<td>University of Wollongong, Australia</td>
</tr>
<tr>
<td>Tsuyoshi Takagi</td>
<td>Future University Hakodate, Japan</td>
</tr>
<tr>
<td>Bogdan Warinschi</td>
<td>Universtiy of Bristol, UK</td>
</tr>
<tr>
<td>Andreas Wespi</td>
<td>IBM Zurich Research Laboratory, Switzerland</td>
</tr>
<tr>
<td>Duncan S. Wong</td>
<td>City University of Hong Kong, China</td>
</tr>
<tr>
<td>Yongdong Wu</td>
<td>Institute for Infocom Research, Singapore</td>
</tr>
<tr>
<td>Alec Yasinsac</td>
<td>Florida State University, USA</td>
</tr>
<tr>
<td>Moti Yung</td>
<td>Columbia University, USA</td>
</tr>
</tbody>
</table>
Yuliang Zheng  
Jianying Zhou  
Sencun Zhu  

University of North Carolina at Charlotte, USA  
Institute for Infocomm Research, Singapore  
Penn State University, USA

Organising Committee

Andrew Brown  
Hasan Qunoo  
Ben Smyth  
Guilin Wang  

University of Birmingham, UK  
University of Birmingham, UK  
University of Birmingham, UK  
University of Birmingham, UK

Publication Chairs

Ben Smyth  
Guilin Wang  

University of Birmingham, UK  
University of Birmingham, UK

External Reviewers

Isaac Agudo  
Cristina Alcaraz  
Man Ho Au  
Jean-Philippe Aumasson  
Vicente Benjumea  
Shaoqing 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 Hrițcu  
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  
Ben Han  
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  
Bo Sheng  
Nicholas Sheppard  
SeongHan Shin  
Taizo Shirai  
Leonie Simpson  
Hui Song  
Graham Steel  
Makoto Sugita  
Ashwin Swaminathan  
Chiu Tan  
Hitoshi Tanuma
<table>
<thead>
<tr>
<th>Alberto Trombetta</th>
<th>Gaven Watson</th>
<th>Yanjiang Yang</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ivan Visconti</td>
<td>Jian Weng</td>
<td>Ng Ching Yu</td>
</tr>
<tr>
<td>Yongtao Wang</td>
<td>Zhe Xia</td>
<td>Rui Zhang</td>
</tr>
<tr>
<td>Xinran Wang</td>
<td>Liang Xie</td>
<td>Jinmin Zhong</td>
</tr>
<tr>
<td>Haodong Wang</td>
<td>Fengyuan Xu</td>
<td>Jakub Zimmermann</td>
</tr>
<tr>
<td>Qihua Wang</td>
<td>Guomin Yang</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

## Invited Talk

Attestation: Evidence and Trust ................................. 1

*George Coker, Joshua Guttman, Peter Loscocco, Justin Sheehy, and Brian Sniffen*

## Authentication

A Novel Solution for End-to-End Integrity Protection in Signed PGP Mail.................................................. 19

*Lijun Liao and Jörg Schwenk*

Unclonable Lightweight Authentication Scheme ...................... 33

*Ghaith Hammouri, Erdinç Öztürk, Berk Birand, and Berk Sunar*

Threat Modelling in User Performed Authentication ................. 49

*Xun Dong, John A. Clark, and Jeremy L. Jacob*

Access with Fast Batch Verifiable Anonymous Credentials ........ 65

*Ke Zeng*

## Side Channel Analysis

Quantifying Timing Leaks and Cost Optimisation .................. 81

*Alessandra Di Pierro, Chris Hankin, and Herbert Wiklicky*

Method for Detecting Vulnerability to Doubling Attacks .......... 97

*Chong Hee Kim and Jean-Jacques Quisquater*

Side Channel Analysis of Some Hash Based MACs: A Response to SHA-3 Requirements ........................................... 111

*Praveen Gauravaram and Katsuyuki Okeya*

## Cryptanalysis

Key Recovery Attack on Stream Cipher Mir-1 Using a Key-Dependent S-Box ......................................................... 128

*Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, and Tomoyasu Suzaki*

Analysis of Two Attacks on Reduced-Round Versions of the SMS4 . . . 141

*Deniz Toz and Orr Dunkelman*
Applying Time-Memory-Data Trade-Off to Meet-in-the-Middle Attack .......................................................... 157  
   Jiali Choy, Khoongming Khoo, and Chuan-Wen Loe

Access Control

Beyond User-to-User Access Control for Online Social Networks ........... 174  
   Mohamed Shehab, Anna Cinzia Squicciarini, and Gail-Joon Ahn

Revocation Schemes for Delegation Licences ........................................ 190  
   Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens,  
   Nora Cuppens-Boulahia, and Adel Bouhoula

Reusability of Functionality-Based Application Confinement Policy Abstractions ............................................................... 206  
   Z. Cliffe Schreuders and Christian Payne

Towards Role Based Trust Management without Distributed Searching of Credentials ......................................................... 222  
   Gang Yin, Huaimin Wang, Jianquan Ouyang, Ning Zhou, and  
   Dianxi Shi

Software Security

BinHunt: Automatically Finding Semantic Differences in Binary Programs .......................................................... 238  
   Debin Gao, Michael K. Reiter, and Dawn Song

Enhancing Java ME Security Support with Resource Usage Monitoring .......................................................... 256  
   Alessandro Castrucci, Fabio Martinelli, Paolo Mori, and  
   Francesco Roperti

Pseudo-randomness Inside Web Browsers ........................................ 267  
   Zhi Guan, Long Zhang, Zhong Chen, and Xianghao Nan

System Security

Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data ........................................ 279  
   Henrich C. Pöhls

Embedding Renewable Cryptographic Keys into Continuous Noisy Data ......................................................... 294  
   Ileana Buhan, Jeroen Doumen, Pieter Hartel, Qiang Tang, and  
   Raymond Veldhuis
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Device Pairing for Asymmetric Pairing Scenarios</td>
<td>311</td>
</tr>
<tr>
<td>Nitesh Saxena and Md. Borhan Uddin</td>
<td></td>
</tr>
<tr>
<td><strong>Applied Cryptography</strong></td>
<td></td>
</tr>
<tr>
<td>Algebraic Description and Simultaneous Linear Approximations of</td>
<td>328</td>
</tr>
<tr>
<td>Addition in Snow 2.0.</td>
<td></td>
</tr>
<tr>
<td>Nicolas T. Courtois and Blandine Debraize</td>
<td></td>
</tr>
<tr>
<td>Towards an Information Theoretic Analysis of Searchable Encryption</td>
<td>345</td>
</tr>
<tr>
<td>Saeed Sedghi, Jeroen Doumen, Pieter Hartel, and Willem Jonker</td>
<td></td>
</tr>
<tr>
<td>A Bootstrap Attack on Digital Watermarks in the Frequency Domain</td>
<td>361</td>
</tr>
<tr>
<td>Sam Behseta, Charles Lam, and Robert L. Webb</td>
<td></td>
</tr>
<tr>
<td>Improved Data Hiding Technique for Shares in Extended Visual Secret</td>
<td>376</td>
</tr>
<tr>
<td>Sharing Schemes</td>
<td></td>
</tr>
<tr>
<td>Rabia Sirhindi, Saeed Murtaza, and Mehreen Afzal</td>
<td></td>
</tr>
<tr>
<td><strong>Security Protocols</strong></td>
<td></td>
</tr>
<tr>
<td>Efficient Multi-authorizer Accredited Symmetrically Private</td>
<td>387</td>
</tr>
<tr>
<td>Information Retrieval</td>
<td></td>
</tr>
<tr>
<td>Mohamed Layouni, Maki Yoshida, and Shingo Okamura</td>
<td></td>
</tr>
<tr>
<td>Specification of Electronic Voting Protocol Properties Using ADM</td>
<td>403</td>
</tr>
<tr>
<td>Logic: FOO Case Study</td>
<td></td>
</tr>
<tr>
<td>Mehdi Talbi, Benjamin Morin, Valérie Viet Triem Tong, Adel Bouhoula,</td>
<td></td>
</tr>
<tr>
<td>and Mohamed Mejri</td>
<td></td>
</tr>
<tr>
<td>Publicly Verifiable Remote Data Integrity</td>
<td>419</td>
</tr>
<tr>
<td>Ke Zeng</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>435</td>
</tr>
</tbody>
</table>