

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, 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

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

Information and Communications Security

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

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

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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

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

Table of Contents

Invited Talks

How to Steal a Botnet and What Can Happen When You Do.....	1
<i>Richard A. Kemmerer</i>	
A User-Mode-Kernel-Mode Co-operative Architecture for Trustable Computing.....	2
<i>Wenbo Mao</i>	

Cryptanalysis

Security Evaluation of a DPA-Resistant S-Box Based on the Fourier Transform	3
<i>Yang Li, Kazuo Sakiyama, Shinichi Kawamura, Yuichi Komano, and Kazuo Ohta</i>	
Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher.....	17
<i>Wenling Wu, Lei Zhang, Liting Zhang, and Wentao Zhang</i>	

Algorithms and Implementations

The RAKAPOSHI Stream Cipher	32
<i>Carlos Cid, Shinsaku Kiyomoto, and Jun Kurihara</i>	
Design of Reliable and Secure Multipliers by Multilinear Arithmetic Codes	47
<i>Zhen Wang, Mark Karpovsky, Berk Sunar, and Ajay Joshi</i>	
Hardware/Software Co-design of Public-Key Cryptography for SSL Protocol Execution in Embedded Systems.....	63
<i>Manuel Koschuch, Johann Großschädl, Dan Page, Philipp Grabher, Matthias Hudler, and Michael Krüger</i>	

Public Key Cryptography

Online/Offline Ring Signature Scheme	80
<i>Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou</i>	
Policy-Controlled Signatures.....	91
<i>Pairat Thorncharoensri, Willy Susilo, and Yi Mu</i>	

Public Key Encryption without Random Oracle Made Truly
 Practical 107
Puwen Wei, Xiaoyun Wang, and Yuliang Zheng

A Public-Key Traitor Tracing Scheme with an Optimal Transmission
 Rate 121
Yi-Ruei Chen and Wen-Guey Tzeng

Security Applications

Computationally Secure Hierarchical Self-healing Key Distribution for
 Heterogeneous Wireless Sensor Networks 135
Yanjiang Yang, Jianying Zhou, Robert H. Deng, and Feng Bao

Enabling Secure Secret Updating for Unidirectional Key Distribution
 in RFID-Enabled Supply Chains 150
*Shaoying Cai, Tieyan Li, Changshe Ma, Yingjiu Li, and
 Robert H. Deng*

Biometric-Based Non-transferable Anonymous Credentials 165
Marina Blanton and William M.P. Hudelson

Software Security

Secure Remote Execution of Sequential Computations 181
Ghassan O. Karame, Mario Strasser, and Srdjan Čapkun

Architecture- and OS-Independent Binary-Level Dynamic Test
 Generation 198
Gen Li, Kai Lu, Ying Zhang, Xicheng Lu, and Wei Zhang

System Security

Measuring Information Flow in Reactive Processes 211
Chunyan Mu

Trusted Isolation Environment: An Attestation Architecture with
 Usage Control Model 226
*Anbang Ruan, Qingni Shen, Liang Gu, Li Wang, Lei Shi,
 Yahui Yang, and Zhong Chen*

Denial-of-Service Attacks on Host-Based Generic Unpackers 241
Limin Liu, Jiang Ming, Zhi Wang, Debin Gao, and Chunfu Jia

Network Security

Predictive Pattern Matching for Scalable Network Intrusion
 Detection 254
Lucas Vespa, Mini Mathew, and Ning Weng

Deterministic Finite Automata Characterization for Memory-Based Pattern Matching	268
<i>Lucas Vespa and Ning Weng</i>	
A LoSS Based On-line Detection of Abnormal Traffic Using Dynamic Detection Threshold	283
<i>Zhengmin Xia, Songnian Lu, Jianhua Li, and Aixin Zhang</i>	
User-Assisted Host-Based Detection of Outbound Malware Traffic	293
<i>Huijun Xiong, Prateek Malhotra, Deian Stefan, Chehai Wu, and Danfeng Yao</i>	
Assessing Security Risk to a Network Using a Statistical Model of Attacker Community Competence	308
<i>Tomas Olsson</i>	

Short Papers I

Using the (Open) Solaris Service Management Facility as a Building Block for System Security	325
<i>Christoph Schuba</i>	
IntFinder: Automatically Detecting Integer Bugs in x86 Binary Program	336
<i>Ping Chen, Hao Han, Yi Wang, Xiaobin Shen, Xinchun Yin, Bing Mao, and Li Xie</i>	
A Comparative Study of Privacy Mechanisms and a Novel Privacy Mechanism	346
<i>Gunmeet Singh and Sarbjeet Singh</i>	

Database Security

Collusion-Resistant Protocol for Privacy-Preserving Distributed Association Rules Mining	359
<i>Xin-Jing Ge and Jian-Ming Zhu</i>	
GUC-Secure Join Operator in Distributed Relational Database	370
<i>Yuan Tian and Hao Zhang</i>	

Trust Management

TSM-Trust: A Time-Cognition Based Computational Model for Trust Dynamics	385
<i>Guangquan Xu, Zhiyong Feng, Xiaohong Li, Hutong Wu, Yongxin Yu, Shizhan Chen, and Guozheng Rao</i>	

Bring Efficient Connotation Expressible Policies to Trust Management 396
Yan Zhang, Zhengde Zhai, and Dengguo Feng

A User Trust-Based Collaborative Filtering Recommendation Algorithm..... 411
Fuzhi Zhang, Long Bai, and Feng Gao

Applied Cryptography

Fingerprinting Attack on the Tor Anonymity System 425
Yi Shi and Kanta Matsuura

Proactive Verifiable Linear Integer Secret Sharing Scheme 439
Chuangui Ma and Xiaofei Ding

A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach 449
Mitra Fatemi, Taraneh Eghlidos, and Mohammadreza Aref

Digital Audio Watermarking Technique Using Pseudo-Zernike Moments 459
Xiangyang Wang, Tianxiao Ma, and Panpan Niu

Short Papers II

An Image Sanitizing Scheme Using Digital Watermarking 474
Masatoshi Noguchi, Manabu Inuma, Rie Shigetomi, and Hideki Imai

Adaptive and Composable Oblivious Transfer Protocols..... 483
Huafei Zhu and Feng Bao

Discrete-Log-Based Additively Homomorphic Encryption and Secure WSN Data Aggregation..... 493
Licheng Wang, Lihua Wang, Yun Pan, Zonghua Zhang, and Yixian Yang

Author Index 503