Lecture Notes in Computer Science 5927

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
Information and Communications Security

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

Springer
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
VIII Organization

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
Yingju 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 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 Chuanglou 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-Bulbaut 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

*Richard A. Kemmerer*

A User-Mode-Kernel-Mode Co-operative Architecture for Trustable Computing

*Wenbo Mao*

## Cryptanalysis

Security Evaluation of a DPA-Resistant S-Box Based on the Fourier Transform

*Yang Li, Kazuo Sakiyama, Shinichi Kawamura, Yuichi Komano, and Kazuo Ohta*

Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher

*Wenling Wu, Lei Zhang, Liting Zhang, and Wentao Zhang*

## Algorithms and Implementations

The RAKAPOSHE Stream Cipher

*Carlos Cid, Shinsaku Kiyomoto, and Jun Kurihara*

Design of Reliable and Secure Multipliers by Multilinear Arithmetic Codes

*Zhen Wang, Mark Karpovsky, Berk Sunar, and Ajay Joshi*

Hardware/Software Co-design of Public-Key Cryptography for SSL Protocol Execution in Embedded Systems

*Manuel Koschuch, Johann Großschädl, Dan Page, Philipp Grabher, Matthias Hudler, and Michael Krüger*

## Public Key Cryptography

Online/Offline Ring Signature Scheme

*Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou*

Policy-Controlled Signatures

*Pairat Thorncharoensri, Willy Susilo, and Yi Mu*
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 Ćapkun*

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*
### Table of Contents

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

### Short Papers I

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

### Database Security

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collusion-Resistant Protocol for Privacy-Preserving Distributed</td>
<td>359</td>
</tr>
<tr>
<td>Association Rules Mining</td>
<td></td>
</tr>
<tr>
<td><em>Xin-Jing Ge and Jian-Ming Zhu</em></td>
<td></td>
</tr>
<tr>
<td>GUC-Secure Join Operator in Distributed Relational Database</td>
<td>370</td>
</tr>
<tr>
<td><em>Yuan Tian and Hao Zhang</em></td>
<td></td>
</tr>
</tbody>
</table>

### Trust Management

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSM-Trust: A Time-Cognition Based Computational Model for Trust</td>
<td>385</td>
</tr>
<tr>
<td>Dynamics</td>
<td></td>
</tr>
<tr>
<td>*Guangquan Xu, Zhiyong Feng, Xiaohong Li, Hutong Wu, Yongxin Yu,</td>
<td></td>
</tr>
<tr>
<td>Shizhan Chen, and Guozheng Rao*</td>
<td></td>
</tr>
</tbody>
</table>
**Table of Contents**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bring Efficient Connotation Expressible Policies to Trust Management</td>
<td>396</td>
</tr>
<tr>
<td><strong>Yan Zhang, Zhengde Zhai, and Dengguo Feng</strong></td>
<td></td>
</tr>
<tr>
<td>A User Trust-Based Collaborative Filtering Recommendation Algorithm</td>
<td>411</td>
</tr>
<tr>
<td><strong>Fuzhi Zhang, Long Bai, and Feng Gao</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Applied Cryptography**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprinting Attack on the Tor Anonymity System</td>
<td>425</td>
</tr>
<tr>
<td><strong>Yi Shi and Kanta Matsuura</strong></td>
<td></td>
</tr>
<tr>
<td>Proactive Verifiable Linear Integer Secret Sharing Scheme</td>
<td>439</td>
</tr>
<tr>
<td><strong>Chuangui Ma and Xiaofei Ding</strong></td>
<td></td>
</tr>
<tr>
<td>A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach</td>
<td>449</td>
</tr>
<tr>
<td><strong>Mitra Fatemi, Taraneh Eghlidos, and Mohammadreza Aref</strong></td>
<td></td>
</tr>
<tr>
<td>Digital Audio Watermarking Technique Using Pseudo-Zernike Moments</td>
<td>459</td>
</tr>
<tr>
<td><strong>Xiangyang Wang, Tianxiao Ma, and Panpan Niu</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Short Papers II**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Image Sanitizing Scheme Using Digital Watermarking</td>
<td>474</td>
</tr>
<tr>
<td><strong>Masatoshi Noguchi, Manabu Inuma, Rie Shigetomi, and Hideki Imai</strong></td>
<td></td>
</tr>
<tr>
<td>Adaptive and Composable Oblivious Transfer Protocols</td>
<td>483</td>
</tr>
<tr>
<td><strong>Huafei Zhu and Feng Bao</strong></td>
<td></td>
</tr>
<tr>
<td>Discrete-Log-Based Additively Homomorphic Encryption and Secure WSN Data Aggregation</td>
<td>493</td>
</tr>
<tr>
<td><strong>Licheng Wang, Lihua Wang, Yun Pan, Zonghua Zhang, and Yixian Yang</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Author Index**                                                     | 503  |