

*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 for Informatics, Saarbruecken, Germany*

Liqun Chen Moti Yung  
Liehuang Zhu (Eds.)

# Trusted Systems

Third International Conference  
INTRUST 2011  
Beijing, China, November 27-29, 2011  
Revised Selected Papers

## Volume Editors

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

Moti Yung  
Columbia University  
Computer Science Department  
S.W. Mudd Building  
New York, NY 10027, USA  
E-mail: my123@columbia.edu

Liehuang Zhu  
Beijing Institute of Technology  
Beijing Key Lab of Intelligent  
Information Technology  
100081 Beijing, China  
E-mail: liehuangz@bit.edu.cn

ISSN 0302-9743  
ISBN 978-3-642-32297-6  
DOI 10.1007/978-3-642-32298-3

e-ISSN 1611-3349  
e-ISBN 978-3-642-32298-3

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012943158

CR Subject Classification (1998): D.4.6, E.3, K.6.5, C.2, K.4.4, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

These proceedings contains the 21 papers presented at the INTRUST 2011 conference, held in Beijing, China, in November 2011. INTRUST 2011 was the third international conference on the theory, technologies, and applications of trusted systems. It was devoted to all aspects of trusted computing systems, including trusted modules, platforms, networks, services, and applications, from their fundamental features and functionalities to design principles, architecture and implementation technologies. The goal of the conference was to bring academic and industrial researchers, designers, and implementers together with end-users of trusted systems, in order to foster the exchange of ideas in this challenging and fruitful area.

INTRUST 2011 built on the successful INTRUST 2009 and INTRUST 2010 conferences, held in Beijing in December 2009 and December 2010, respectively. The proceedings of INTRUST 2009, containing 16 papers, were published in volume 6163 of the *Lecture Notes in Computer Science*. The proceedings of INTRUST 2010, containing 23 papers, were published in volume 6802 of the *Lecture Notes in Computer Science*.

Apart from the 21 contributed papers, the program of INTRUST 2011 also consisted of a workshop, titled “Asian Lounge on Trust, Security and Privacy.” The workshop included six keynote speeches from Yanan Hu (Broadband Wireless IP Standard Group and China IWNCOMM Co., Ltd.), Wenbo Mao (Daoli Limited), Graeme Proudler (Hewlett-Packard Laboratories and TCG), Kouichi Sakurai (Kyushu University), Moti Yung (Columbia University and Google), and Huanguo Zhang (Wuhan University). Special thanks are due to these speakers.

The contributed papers were selected from 34 submissions from 18 countries. All submissions were blind-reviewed, i.e., the Program Committee members provided reviews on anonymous submissions. The refereeing process was rigorous, involving on average three (and mostly more) independent reports being prepared for each submission. The individual reviewing phase was followed by profound discussions about the papers, which contributed greatly to the quality of the final selection. A number of accepted papers were shepherded by some Program Committee members in order to make sure the review comments were addressed properly. We are very grateful to our hard-working and distinguished Program Committee for doing such an excellent job in a timely fashion.

For the proceedings the papers have been divided into seven main categories, namely, trusted services, mobile trusted systems, trusted networks, security analysis, cryptographic aspects, implementation, and anonymous direct attestation.

We also want to thank the conference Steering Committee organized by Yongfei Han, the conference General Chairs, Robert Deng, Heyan Huang and Chris Mitchell, the Organizing Chair Liehuang Zhu, and Publicity Chairs, Xuhua Ding, and Lejian Liao, for valuable guidance and assistance and for handling the

arrangements in Beijing. Thanks are also due to EasyChair for providing the submission and review webserver and to Guoyong Cheng for maintaining the conference webpage.

On behalf of the conference organization and participants, we would like to express our appreciation to Beijing Institute of Technology, ONETS Wireless & Internet Security Company, Singapore Management University, and the Administrative Committee of Zhongguangcun Haidian Science Park for their generous sponsorship of this event.

We would also like to thank all the authors who submitted their papers to the INTRUST 2011 conference, all external referees, and all the attendees of the conference. Authors of accepted papers are thanked again for revising their papers according to the feedback from the conference participants. The revised versions were not checked by the Program Committee, so authors bear full responsibility for their contents. We thank the staff at Springer for their help with producing the proceedings.

February 2012

Liqun Chen  
Moti Yung  
Lihuang Zhu

# INTRUST 2011

**The Third International Conference on Trusted Systems**  
**Beijing, P.R. China**  
**November 27–29, 2011**

*Sponsored by*  
*Beijing Institute of Technology*  
*ONETS Wireless & Internet Security Company*  
*Singapore Management University*  
*The Administrative Committee of Zhongguangcun Haidian Science Park*

## General Chairs

Robert Deng	Singapore Management University, Singapore
Heyan Huang	Beijing Institute of Technology, China
Chris Mitchell	Royal Holloway, University of London, UK

## Program Chairs

Liqun Chen	Hewlett-Packard Laboratories, UK
Moti Yung	Columbia University and Google Inc., USA
Liehuang Zhu	Beijing Institute of Technology, China

## Program Committee

Endre Bangerter	Bern University of Applied Sciences, Switzerland
Boris Balacheff	HP Laboratories, UK
Feng Bao	I2R, Singapore
Kefei Chen	Shanghai Jiaotong University, China
Haibo Chen	Fudan University, China
Zhen Chen	Tsinghua University, China
Zhong Chen	Peking University, China
Xuhua Ding	Singapore Management University, Singapore
Kurt Dietrich	Graz University of Technology, Austria
Loïc Duflet	SGDN, France
Dengguo Feng	Chinese Academy of Sciences, China
Dieter Gollmann	Hamburg University of Technology, Germany
David Grawrock	Intel, USA

Sigrid Guürgens	Fraunhofer Institute for Secure Information Technology, Germany
Weili Han	Fudan University, China
Dirk Kuhlmann	HP Laboratories, UK
Xuejia Lai	Shanghai Jiaotong University, China
Jiangtao Li	Intel, USA
Shujun Li	University of Konstanz, Germany
Peter Lipp	Graz University of Technology, Austria
Javier Lopez	University of Malaga, Spain
Andrew Martin	University of Oxford, UK
Shin'ichiro Matsuo	NICT, Japan
Chris Mitchell	RHUL, UK
Yi Mu	University of Wollongong, Australia
David Naccache	ENS, France
Raphael Phan	Loughborough University, UK
Bart Preneel	KU Leuven, Belgium
Graeme Proudler	HP Laboratories, UK
Sihan Qing	Chinese Academy of Sciences, China
Emily Ratliff	IBM, USA
Scott Rotondo	Oracle, USA
Ahmad-Reza Sadeghi	Technical University Darmstadt and Fraunhofer SIT Darmstadt, Germany
Kouichi Sakurai	Kyushu University, Japan
Wenchang Shi	Renmin University, China
Willy Susilo	University of Wollongong, Australia
Qiang Tang	University of Twente, The Netherlands
Claire Vishik	Intel, USA
Guilin Wang	University of Wollongong, Australia
Jian Weng	Jinan University, China
Shouhuai Xu	UTSA, USA
Rui Xue	Chinese Academy of Sciences, China
Huanguo Zhang	Wuhan University, China
Xing Zhang	BJUT, China
Xinwen Zhang	Huawei Research Center, USA
Yongbin Zhou	Chinese Academy of Sciences, China
Yan Zhou	Peking University, China

## Steering Committee

Liqun Chen	HP Laboratories, UK
Robert Deng	SMU, Singapore
Yongfei Han	BJUT and ONETS, China
Chris Mitchell	RHUL, UK
Moti Yung	Google and Columbia University, USA

## Organizing Chair

Liehuang Zhu

Beijing Institute of Technology, China

## Publication Chairs

Xuhua Ding

Singapore Management University, Singapore

Lejian Liao

Beijing Institute of Technology, China

## External Reviewers

Yuichi Asahiro

Yizhi Ren

Man Ho Au

Thomas Schneider

Andreas Fuchs

Jae Hong Seo

Wei Gao

Isamu Teranishi

Yun Huang

Yasuyuki Tsukada

Tingting Lin

Ronald Tögl

Yu Long

Christian Wachsmann

Yiyuan Luo

Liangliang Wang

Bart Mennink

Laiping Zhao

Mridul Nandi



# Table of Contents

## Trusted Services

A Flexible Software Development and Emulation Framework for ARM TrustZone.....	1
<i>Johannes Winter, Paul Wiecele, Martin Pirker, and Ronald Tögl</i>	
Building General Purpose Security Services on Trusted Computing.....	16
<i>Chunhua Chen, Chris J. Mitchell, and Shaohua Tang</i>	
Enforcing Sticky Policies with TPM and Virtualization.....	32
<i>Gina Kouna and Liqun Chen</i>	

## Mobile Trusted Systems

Mass Transit Ticketing with NFC Mobile Phones.....	48
<i>Jan-Erik Ekberg and Sandeep Tamrakar</i>	
Anonymous Ticketing for NFC-Enabled Mobile Phones.....	66
<i>David Derler, Klaus Potzmader, Johannes Winter, and Kurt Dietrich</i>	

## Security Analysis

Some Improvements to the Cost-Based Framework for Analyzing Denial of Service Attacks.....	84
<i>Qinggang Yue, Feng Liu, and Rui Xue</i>	
Fault Detection of the MacGuffin Cipher against Differential Fault Attack.....	102
<i>Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu, and Xiaohu Huang</i>	
Computationally Sound Symbolic Analysis of EAP-TNC Protocol.....	113
<i>Zijian Zhang, Liehuang Zhu, Feng Wang, Lejian Liao, Cong Guo, and Hongyuan Wang</i>	
A Technique for Remote Detection of Certain Virtual Machine Monitors.....	129
<i>Christopher Jämthagen, Martin Hell, and Ben Smeets</i>	

## Cryptographic Aspects

Indifferentiability of Domain Extension Modes for Hash Functions.....	138
<i>Yiyuan Luo, Xuejia Lai, and Zheng Gong</i>	

Multicollisions and Graph-Based Hash Functions . . . . .	156
<i>Kimmo Halunen</i>	
A General, Flexible and Efficient Proof of Inclusion and Exclusion . . . . .	168
<i>Kun Peng</i>	
MQQ-SIG: An Ultra-Fast and Provably CMA Resistant Digital Signature Scheme . . . . .	184
<i>Danilo Gligoroski, Rune Steinsmo Ødegård, Rune Erlend Jensen, Ludovic Perret, Jean-Charles Faugère, Svein Johan Knapskog, and Smile Markovski</i>	
Multifactor Authenticated Key Renewal . . . . .	204
<i>Shin'ichiro Matsuo, Daisuke Moriyama, and Moti Yung</i>	
Restricted Identification Scheme and Diffie-Hellman Linking Problem . . .	221
<i>Miroslaw Kutylowski, Lukasz Krzywiecki, Przemysław Kubiak, and Michał Koza</i>	
<b>Trusted Networks</b>	
Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks . . . . .	239
<i>Dong Hao, Avishek Adhikari, and Kouichi Sakurai</i>	
Hash Chains at the Basis of a Secure Reactive Routing Protocol . . . . .	258
<i>Thouraya Bouabana-Tebibel</i>	
<b>Implementation</b>	
Evaluation of a PUF Device Authentication Scheme on a Discrete 0.13um SRAM . . . . .	271
<i>Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik, and Marcin Wójcik</i>	
A Performance Analysis of Identity-Based Encryption Schemes . . . . .	289
<i>Pengqi Cheng, Yan Gu, Zihong Lv, Jianfei Wang, Wenlei Zhu, Zhen Chen, and Jiwei Huang</i>	
<b>Direct Anonymous Attestation</b>	
A (Corrected) DAA Scheme Using Batch Proof and Verification . . . . .	304
<i>Ernie Brickell, Liqun Chen, and Jiangtao Li</i>	
DAA Protocol Analysis and Verification . . . . .	338
<i>Yu Qin, Xiaobo Chu, Dengguo Feng, and Wei Feng</i>	
<b>Author Index</b> . . . . .	351