

*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 (Eds.)

# Trusted Systems

Second International Conference, INTRUST 2010  
Beijing, China, December 13-15, 2010  
Revised Selected Papers

## Volume Editors

Liqun Chen  
Hewlett-Packard Labs  
Long Down Avenue  
Stoke Gifford  
Bristol BS34 8QZ, 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

ISSN 0302-9743  
ISBN 978-3-642-25282-2  
DOI 10.1007/978-3-642-25283-9  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-25283-9

Library of Congress Control Number: 2011941150

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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](http://www.springer.com))

# Preface

These proceedings contains the 23 papers presented at the INTRUST 2010 conference, held in Beijing, China, in December 2010. INTRUST 2010 was the second 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 2010 built on the successful INTRUST 2009 conference, also held in Beijing in December 2009. The proceedings of INTRUST 2009, containing 16 papers, were published in volume 6163 of the *Lecture Notes in Computer Science* series.

The program consisted of a workshop with nine invited talks and 23 contributed papers. The workshop, titled “Asian Lounge on Trust, Security and Privacy”, included the distinguished keynote speaker Andrew Yao (Tsinghua University), and four more keynote speakers—Jingtai Ding (University of Cincinnati), Xuejia Lai (Shanghai Jiaotong University), DongHoon Lee (Korea University) and Claire Vishik (Intel)—along with talks by Liqun Chen (HP Labs), Shujun Li (University of Konstanz), Ahmad-Reza Sadeghi (TU Darmstadt and Fraunhofer SIT) and Moti Yung (Google). Special thanks are due to these speakers and also to Ahmad-Reza Sadeghi for his initiation and organization of the workshop.

The contributed papers were selected from 66 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 at least 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 a lot 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. We believe that the result is a high-quality set of papers, some of which have been significantly improved as a result of the refereeing process.

For these proceedings the papers have been divided into seven main categories, namely, implementation technology, security analysis, cryptographic aspects, mobile trusted systems, hardware security, attestation, and software protection.

We also want to thank the conference General Chairs, Robert Deng, Yongfei Han and Chris Mitchell, the Organizing Chair Jian Li, and Publicity Chairs, Xuhua Ding, and Xing Zhang, for valuable assistance and for handling the arrangements in Beijing. Thanks are also due to easyChair for providing the submission and review webserver and to Yang Zhen for designing and maintaining the conference website.

We would also like to thank all the authors who submitted their papers to the INTRUST 2010 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, and so authors bear full responsibility for their contents. We thank the staff at Springer for their help with producing the proceedings.

February 2011

Liqun Chen  
Moti Yung

# INTRUST 2010

**The Second International Conference on Trusted Systems**

**Beijing, P.R. China  
December 13–15, 2010**

*Sponsored by  
Beijing University 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
Yongfei Han	Beijing University of Technology and ONETS, 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

## **Program Committee**

N. Asokan	Nokia Research Center, Finland
Endre Bangerter	Bern University of Applied Sciences, Switzerland
Boris Balacheff	HP Laboratories, UK
Feng Bao	I2R, Singapore
Kefei Chen	Shanghai Jiaotong University, China
Zhen Chen	Tsinghua University, China
Zhong Chen	Peking University, China
James Davenport	University of Bath, UK
Xuhua Ding	Singapore Management University, Singapore
Loïc Duflot	SGDN, France
Dieter Gollmann	Hamburg University of Technology, Germany
David Grawrock	Intel, USA

Sigrid Grgens	Fraunhofer Institute for Secure Information Technology, Germany
Dirk Kuhlmann	HP Laboratories, UK
Xuejia Lai	Shanghai Jiaotong University, China
Jian Li	BJUT, China
Jiangtao Li	Intel, USA
Peter Lipp	Graz University of Technology, Austria
Wenbo Mao	EMC Research, China
Andrew Martin	University of Oxford, 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
Emily Ratliff	IBM, USA
Scott Rotondo	Oracle, USA
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Wenchang Shi	Renmin University, China
Willy Susilo	University of Wollongong, Australia
Qiang Tang	University of Twente, The Netherlands
Vijay Varadharajan	Macquarie University, Australia
Claire Vishik	Intel, USA
Guilin Wang	University of Birmingham, UK
Duncan S. Wong	City University of Hong Kong, China
Shouhuai Xu	UTSA, USA
Xing Zhang	BJUT, China

## Steering Committee

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

## Organizing Chair

Jian Li	Beijing University of Technology, China
---------	---

## Publication Chairs

Xuhua Ding	Singapore Management University, Singapore
Xing Zhang	BJUT, China

## External Reviewers

Akihiro Sakai  
Alexandra Dmitrienko  
Beipeng Mu  
Ben Smyth  
Chris Heunen  
Christian Wachsmann  
Christos Ioannides  
Cornelius Namiluko  
Dalia Khader  
Daniel Hein  
Daniel Page  
Fagen Li  
Feng Xie  
Fuchun Guo  
Gideon Bibu  
Hans Löhr  
Jens Hermans  
Jessica Jones  
Jian Weng  
Jinli Meng  
Johannes Winter  
John Lyle  
Joseph Liu  
Kurt Dietrich  
Man Ho Au  
Marcel Winandy  
Martin Pirker  
Masakazu Soshi  
Nicky Mouha

Nicolai Kunzte  
Qingji Zheng  
Qiong Huang  
Rehana Yasmin  
Roderick Bloem  
Roel Peeters  
Ronald Toegl  
Saif Al-Kuwari  
Sebastian Faust  
Shoichi Hirose  
Steffen Schulz  
Stephan Krenn  
Tsz Hon Yuen  
Unal Kocabas  
Vincent Rijmen  
Wei Gao  
Wei Wu  
Weiqi Dai  
Wook SHIN  
Xianhui Lu  
Xinming Chen  
Yiyuan Luo  
Yizhi Ren  
Yuan Tian  
Yuan Wong  
Zhenxin Zhan  
Zhongmei Wan  
Ziye Yang

# Table of Contents

## Implementation Technology

Seamless Integration of Trusted Computing into Standard Cryptographic Frameworks .....	1
<i>Andreas Reiter, Georg Neubauer, Michael Kapfenberger, Johannes Winter, and Kurt Dietrich</i>	
Design and Implementation of Document Access Control Model Based on Role and Security Policy .....	26
<i>Liangjian Mao, Shuzhen Yao, Kai Zhang, and Kouichi Sakurai</i>	
Towards High-Performance IPsec on Cavium OCTEON Platform .....	37
<i>Jinli Meng, Xinming Chen, Zhen Chen, Chuang Lin, Beipeng Mu, and Lingyun Ruan</i>	

## Security Analysis

An Abstract Model of a Trusted Platform .....	47
<i>Cornelius Namiluko and Andrew Martin</i>	
Modeling TCG-Based Secure Systems with Colored Petri Nets .....	67
<i>Liang Gu, Yao Guo, Yanjiang Yang, Feng Bao, and Hong Mei</i>	
Information Flow Graph: An Approach to Identifying Covert Storage Channels .....	87
<i>Xiangmei Song, Shiguang Ju, Changda Wang, and Conghua Zhou</i>	
Trusted Subjects Configuration Based on TE Model in MLS Systems ...	98
<i>Shangjie Li and Yeping He</i>	

## Cryptographic Aspects (I)

Key Exchange with Anonymous Authentication Using DAA-SIGMA Protocol .....	108
<i>Jesse Walker and Jiangtao Li</i>	
Revocation of Direct Anonymous Attestation .....	128
<i>Liqun Chen and Jiangtao Li</i>	
Measuring Random Tests by Conditional Entropy and Optimal Execution Order .....	148
<i>Jialin Huang and Xuejia Lai</i>	

## Cryptographic Aspects (II)

Leakage Resilient Strong Key-Insulated Signatures in Public Channel . . .	160
<i>Le Trieu Phong, Shin'ichiro Matsuo, and Moti Yung</i>	
Two-Head Dragon Protocol: Preventing Cloning of Signature Keys (Work in Progress) . . . . .	173
<i>Przemysław Błażkiewicz, Przemysław Kubiak, and Mirosław Kutylowski</i>	
Addressing Leakage of Re-encryption Key in Proxy Re-encryption Using Trusted Computing . . . . .	189
<i>Yanjiang Yang, Liang Gu, and Feng Bao</i>	

## Mobile Trusted Systems

Can Hand-Held Computers Still Be Better Smart Cards? . . . . .	200
<i>Sandeep Tamrakar, Jan-Erik Ekberg, Pekka Laitinen, N. Asokan, and Tuomas Aura</i>	
TruWalletM: Secure Web Authentication on Mobile Platforms . . . . .	219
<i>Sven Bugiel, Alexandra Dmitrienko, Kari Kostiaainen, Ahmad-Reza Sadeghi, and Marcel Winandy</i>	
A Game Theory-Based Surveillance Mechanism against Suspicious Insiders in MANETs (Work-in-Progress) . . . . .	237
<i>Dong Hao, Yizhi Ren, and Kouichi Sakurai</i>	

## Hardware Security

Hardware Trojans for Inducing or Amplifying Side-Channel Leakage of Cryptographic Software . . . . .	253
<i>Jean-François Gallais, Johann Großschädl, Neil Hanley, Markus Kasper, Marcel Medwed, Francesco Regazzoni, Jörn-Marc Schmidt, Stefan Tillich, and Marcin Wójcik</i>	
An Emerging Threat: Eve Meets a Robot (Work-in-Progress) . . . . .	271
<i>Kahraman D. Akdemir, Deniz Karakoyunlu, Taskin Padir, and Berk Sunar</i>	

## Attestation

On Leveraging Stochastic Models for Remote Attestation . . . . .	290
<i>Tamleek Ali, Mohammad Nauman, and Xinwen Zhang</i>	

Interoperable Remote Attestation for VPN Environments (Work in Progress) .....	302
<i>Ingo Bente, Bastian Hellmann, Joerg Vieweg, Josef von Helden, and Arne Welzel</i>	
A Novel Reputation Computing Model (Work-in-Progress) .....	316
<i>Yongzhong Zhang, Qi Li, and Zhangxi Lin</i>	
 <b>Software Protection</b>	
acTvSM: A Dynamic Virtualization Platform for Enforcement of Application Integrity .....	326
<i>Ronald Toegl, Martin Pirker, and Michael Gissing</i>	
Software, Vendors and Reputation: An Analysis of the Dilemma in Creating Secure Software .....	346
<i>Craig S. Wright</i>	
<b>Author Index</b> .....	361