Preface

This volume contains the 16 papers presented at the INTRUST 2009 conference, held in Beijing, China in December 2009. INTRUST 2009 was the first 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.

The program consisted of 3 invited talks and 20 contributed papers. The invited speakers were Wenchang Shi (Renmin University of China), David Wooten (Microsoft) and Scott Rotondo (Sun Microsystems). The first speaker provided a paper, which is included in these proceedings. Special thanks are due to these speakers.

The contributed talks were arranged with two main tracks, one devoted to academic aspects of trusted computing systems (addressed by these proceedings), and the other devoted to industrial aspects. The contributed papers were selected out of 42 submissions from 13 countries. The refereeing process was rigorous, involving at least three (and mostly more) independent reports being prepared for each submission. 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, invited talk, secure storage, attestation, trusted network, virtualization, applications, and supporting technology.

We also want to thank the conference General Chairs, Robert Deng and Yongfei Han, the Organizing Chairs, Lijuan Duan and Jian Li, and Publicity Chairs, Xiaona Chen, Xuhua Ding, Sijin Li and Yu Wang, for valuable assistance and handling the arrangements in Beijing. Thanks also 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 2009 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 2010

Liqun Chen
Moti Yung
The International Conference on Trusted Systems

Beijing, P.R. China
December 17–19, 2009

Sponsored by
Beijing University of Technology
Chinese Academy of Engineering
ONETS Wireless & Internet Security Company
Singapore Management University
Trusted Computing Group

General Chairs
Robert Deng  Singapore Management University, Singapore
Yongfei Han  Beijing University of Technology and ONETS, China

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
James Davenport  University of Bath, UK
Xuhua Ding  Singapore Management University, Singapore
Loc Duflot  SGDN, France
Paul England  Microsoft, USA
Dengguo Feng  Chinese Academy of Sciences, China
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
Qing Liang  Ricoh Software Research Center, China
Peter Lipp  Graz University of Technology, Austria
Javier Lopez  University of Malaga, Spain
Wenbo Mao  EMC Research, China
Andrew Martin  University of Oxford, UK
Chris Mitchell  RHUL, UK
Yi Mu  University of Wollongong, Australia
David Naccache  ENS, France
Yoram Ofek  Trento, Italy
Alina Oprea  RSA Laboratories, USA
Kenny Paterson  RHUL, UK
Raphael Phan  Loughborough University, UK
Bart Preneel  KU Leuven, Belgium
Graeme Proudler  HP Laboratories, UK
Sihan Qing  Chinese Academy of Sciences, China
Zulfikar Ramzan  Symantec, USA
Carsten Rudolph  Fraunhofer Institute for Secure Information Technology, Germany
Mark Ryan  University of Birmingham, UK
Ahmad-Reza Sadeghi  Ruhr University Bochum, Germany
Kouichi Sakurai  Kyushu University, Japan
Luis Sarmenta  MIT, USA
Jean-Pierre Seifert  Technical University of Berlin and T-Labs, Germany
Sean Smith  Dartmouth College, USA
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
Steve Weis  Google, USA
Duncan S. Wong  City University of Hong Kong, China
Shouhuai Xu  UTSA, USA
Huanguo Zhang  Wuhan University, China
Xing Zhang  BJUT, 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 Committee

Lijuan Duan  Beijing University of Technology, China
Jian Li  Beijing University of Technology, China

Publication Chairs

Xiaona Chen  ONETS, China
Xuhua Ding  Singapore Management University, Singapore
Sijin Li  ONETS, China
Yu Wang  ONETS, China

External Reviewers

Jean-Philippe Aumasson  John Lyle
Luigi Catuogno  Sandra Marcello
Zhengjie Cheng  Aarthi Nagarajan
Weiqi Dai  Cornelius Namiluko
Zijian Deng  Martin Pirker
Kurt Dietrich  Yu Qin
Ming Duan  Steffen Schulz
Jan-Erik Ekberg  Ronald Tgl
Wei Gao  Kerem Varici
Benedikt Gierlichs  Yongtao Wang
Jun Huh  Marcel Winandy
Qingguang Ji  Qi Xie
Nicolai Kuntze  Wentao Zhang
Shengli Liu  Bo Zhu
Hans Loehr
In December 2009, Prof. Yoram Ofek, a member of the Intrust 2009 program committee, a full professor at the University of Trento, Italy, and a world renowned expert in computer communication networks and trusted computing, passed away after two years of heroic struggle with cancer. In the last two years Yoram kept his good spirit and optimism as always, he continued his duties, his professional commitments and his active work: leading research efforts, helping career development of young colleagues, and supporting the scientific community, in general, and the trusted computing community, in particular, in many ways.

Yoram's outstanding academic career started when he received his B.Sc. degree in electrical engineering from the Technion-Israel Institute of Technology, and then he received his M.Sc. and Ph.D. degrees in electrical engineering from the University of Illinois-Urbana. He then expanded his research while at IBM T. J. Watson Research Center, and for his invention of the MetaRing and his contributions to the SSA storage products, he was awarded the IBM Outstanding Innovation Award. After IBM, he ran his own startup company Synchrodyne, and then got a distinguished award by the European Commission and became “A Marie Curie Chair Professor in Trento,” prior to his appointment as a full professor in the same university.

Professor Ofek’s achievements include 45 USA and European patents and more than 120 journal and conference papers. As a networking expert, he invented six novel architectures for networking, computing and storage: (1) A ring networks with spatial bandwidth reuse with a family of fairness algorithms; (2) An optical hypergraph for combining multiple passive optical stars with burst mode bit synchronization and clock synchronization; (3) The notion of embedding of virtual rings in arbitrary topology networks optimized for distributed computing; (4) Global IP packet switching network, which utilizes UTC and pipeline forwarding to guarantee deterministic operation, optimized for streaming media applications; and (6) Optical fractional lambda switching for WDM networks, optimized for switching scalability. His work on
trusted computing, in turn, centered around the invention of methods for remote au-
thentication (remote entrusting) of software during execution that can be used for
numerous tasks, such as protection of programs run remotely on networks and servers,
distributed, cloud and grid remote executions, and protecting (audio/video) content at
remote users. For his accomplishment Dr. Ofek was elected a fellow of the IEEE.

Yoram was a kind and warm person, passionate about his work and computer sci-
ence and engineering in general, he was highly respected as a friend, colleague, re-
search leader and a teacher. He is mourned by his colleagues, co-workers and students
around the world who wish to extend their deepest sympathy to his wife Barbara his
four children: Tidhar, Gidon, Daphna and Maya, and the rest of his family. We dedi-
cate this conference proceedings volume to his blessed memory.
# Table of Contents

## Invited Talk

On Design of a Trusted Software Base with Support of TPCM .............. 1

*Wenchang Shi*

## Secure Storage

External Authenticated Non-volatile Memory with Lifecycle Management for State Protection in Trusted Computing ................. 16

*Jan-Erik Ekberg and N. Asokan*

A Method for Safekeeping Cryptographic Keys from Memory Disclosure Attacks ......................................................... 39

*T. Paul Parker and Shouhuai Xu*

## Attestation

Remote Attestation on Function Execution ........................................ 60

*Liang Gu, Yueqiang Cheng, Xuhua Ding, Robert H. Deng, Yao Guo, and Weizhong Shao*

Scalable Remote Attestation with Privacy Protection .......................... 73

*Tamleek Ali Tanveer, Masoom Alam, and Mohammad Nauman*

Anonymous Credentials for Java Enabled Platforms: A Performance Evaluation ......................................................... 88

*Kurt Dietrich*

## Trusted Network

SocialClouds: Concept, Security Architecture and Some Mechanisms ....... 104

*Shouhuai Xu and Moti Yung*

Privacy Enhanced Trusted Network Connect ................................. 129

*Ingo Bente, Joerg Vieweg, and Josef von Helden*

Research on Multistage Interconnection Architecture and Collision Detection Model ......................................................... 146

*Mengmeng Li and Yong Zhao*
# Virtualization

Trusted Virtual Domains – Design, Implementation and Lessons  
Learned .................................................. 156  

Luigi Catuogno, Alexandra Dmitrienko, Konrad Eriksson,  
Dirk Kuhlmann, Gianluca Ramunno, Ahmad-Reza Sadeghi,  
Steffen Schulz, Matthias Schunter, Marcel Winandy, and Jing Zhan

Trusted Integrity Measurement and Reporting for Virtualized  
Platforms .................................................. 180  

Serdar Cabuk, Liqun Chen, David Plaquin, and Mark Ryan

# Applications

A Feather-Weight Application Isolation Model ......................... 197  

Jianhua Liao, Yong Zhao, and Changxiang Shen

Exploring Trust of Mobile Applications Based on User Behaviors...... 212  

Zheng Yan, Yan Dong, Valtteri Niemi, and Guoliang Yu

Trusted Firmware Services Based on TPM .......................... 227  

Zhenlong Du, Xiaoli Li, and Kangkang Shen

# Supporting Technology

Improved Cryptanalysis of the FOX Block Cipher ......................... 236  

Zhongming Wu, Yiyuan Luo, Xuejia Lai, and Bo Zhu

Bitwise Higher Order Differential Cryptanalysis .......................... 250  

Bo Zhu, Kefei Chen, and Xuejia Lai

Author Index .................................................. 263