Lecture Notes in Computer Science 6802

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Liqun Chen Moti Yung (Eds.)

Trusted Systems

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

Springer

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 e-ISSN 1611-3349
ISBN 978-3-642-25282-2 e-ISBN 978-3-642-25283-9
DOI 10.1007/978-3-642-25283-9
Springer Heidelberg Dordrecht London New York

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

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 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 (Universtiy 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

Security Analysis

Cryptographic Aspects (I)

Cryptographic Aspects (II)

Mobile Trusted Systems

Hardware Security

Attestation

Software Protection