Lecture Notes in Computer Science 7711

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

Chris J. Mitchell Allan Tomlinson (Eds.)

Trusted Systems

4th International Conference, INTRUST 2012
London, UK, December 17-18, 2012
Proceedings

Springer

Volume Editors

Chris J. Mitchell
Allan Tomlinson
University of London, Information Security Group
Royal Holloway, Egham, Surrey TW20 0EX, UK
E-mail: me@chrismitchell.net, allan.tomlinson@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-35370-3 e-ISBN 978-3-642-35371-0
DOI 10.1007/978-3-642-35371-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: Applied for

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

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

This volume contains ten papers presented and discussed at the InTrust 2012 conference, held at Royal Holloway, University of London, Egham, UK, in December 2012. InTrust 2012 was the fourth 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 functionality 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 2012 built on the three previous successful conferences in the series, held in Beijing in December 2009, December 2010, and November 2011. 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*. The proceedings of INTRUST 2011, containing 21 papers, were published in volume 7222 of the *Lecture Notes in Computer Science*.

The program of InTrust 2012 was made up of six contributed papers, four invited keynote presentations, and a panel session. Short papers by three of the invited speakers (Javier Lopez, Christof Paar, and Mark Ryan) are included in the proceedings; the fourth keynote speaker, Paul Waller (CESG, UK) gave a talk entitled "Secure By Default — Assuring and Evolving Platform Security". The panel session was organized and led by Shin'ichiro Matsuo (NICT, Japan), and a short paper which formed the basis for the session is included in the proceedings. Panel session participants included Nicolai Kuntze (Fraunhofer Institute), Graeme Proudler (Hewlett-Packard Laboratories and TCG), Charles Brookson (Chair of GSMA SG and ETSI OCG), and Kenny Paterson (Royal Holloway, University of London). Special thanks are due to the keynote speakers, the panel session organizer, and the panel session participants.

The contributed papers were selected out of 19 submissions from 14 countries, giving an acceptance rate of 32%. All submissions were blind-reviewed, i.e., the Program Committee members provided reviews on anonymous submissions. The refereeing process was rigorous, involving three (and sometimes more) independent reports being prepared for each submission. The individual reviewing phase was followed by discussions about the papers, which contributed greatly to the quality of the final selection. A number of accepted papers were shepherded by Program Committee members in order to make sure the review comments were properly addressed. We are very grateful to our hard-working and distinguished Program Committee for doing such an excellent job in a timely fashion.

We owe a huge debt to Liqun Chen for acting as General Chair and providing a constant source of helpful advice and encouragement; without her this event would not have taken place. We would also like to thank the conference Steering Committee led by Yongfei Han for valuable guidance and assistance, and Emma Mosley for managing the arrangements at Royal Holloway. Thanks are also due to EasyChair for providing the submission and review Web server.

On behalf of the conference organization and participants, we would like to express our appreciation to Singapore Management University and the Information Security Group at Royal Holloway for their generous sponsorship of this event.

We would also like to thank the authors who submitted their papers to the InTrust 2012 conference, the external referees, and, last but not least, 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 formally checked by the Program Committee, so the authors bear full responsibility for their contents. We thank the staff at Springer for their help with producing the proceedings.

October 2012

Chris Mitchell
Allan Tomlison

InTrust 2012

The 4th International Conference on Trusted Systems
Royal Holloway, University of London, Egham, UK

December 17–18, 2012

Honorary Chairs

Yongfei Han	BJUT and ONETS, China
Moti Yung	Google and Columbia University, USA

General Chairs

Liqun Chen	Hewlett-Packard Laboratories, UK
Chris Mitchell	Royal Holloway, University of London, UK
Allan Tomlinson	Royal Holloway, University of London, UK

Program Chairs

Chris Mitchell	Royal Holloway, University of London, UK
Allan Tomlinson	Royal Holloway, University of London, UK

Program Committee

Endre Bangerter	Bern University of Applied Sciences, Switzerland
Feng Bao	I2R, Singapore
Giampaolo Bella	Università di Catania, Italy
Haibo Chen	Shanghai Jiao Tong University, China
Zhong Chen	Peking University, China
Kurt Dietrich	Graz University of Technology, Austria
Xuhua Ding	Singapore Management University, Singapore
Loic Duflot	SGDN, France
Dieter Gollmann	Hamburg University of Technology, Germany
David Grawrock	Intel, USA
Sigrid Guergens	Fraunhofer Institute for Secure Information Technology, Germany
Dirk Kuhlmann	HP Laboratories, UK
Xuejia Lai	Shanghai Jiao Tong 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
Yi Mu	University of Wollongong, Australia
David Naccache	ENS, France
Kenny Paterson	Royal Holloway, University of London, UK
Graeme Proudler	HP Laboratories, UK
Sihan Qing	Chinese Academy of Sciences, China
Scott Rotondo	Oracle, USA
Mark Ryan	University of Birmingham, UK
Willy Susilo	University of Wollongong, Australia
Qiang Tang	University of Twente, The Netherlands
Claire Vishik	Intel, USA
Jian Weng	Jinan University, China
Shouhuai Xu	UTSA, USA
Rui Xue	Chinese Academy of Sciences, China
Xinwen Zhang	Huawei Research Center, USA
Yongbin Zhou	Chinese Academy of Sciences, China
Liehuang Zhu	Beijing Institute of Technology, China
Yan Zhu	Peking University, China

Steering Committee

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

External Reviewers

Sergiu Bursuc
Liqun Chen
Ulrich Fiedler
Qi Li
Lei Liu
Weiliang Luo
Li Yang
Rui Zhang
Qingji Zheng

Table of Contents

Session 6: Embedded Security