

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Liqun Chen Chris J. Mitchell
Andrew Martin (Eds.)

Trusted Computing

Second International Conference, Trust 2009
Oxford, UK, April 6-8, 2009
Proceedings



Springer

Volume Editors

Liqun Chen

Hewlett-Packard Laboratories

Filton Road, Stoke Gifford, Bristol BS34 8QZ, UK

E-mail: liqun.chen@hp.com

Chris J. Mitchell

Royal Holloway, University of London

Information Security Group

Egham, Surrey TW20 0EX, UK

E-mail: c.mitchell@rhul.ac.uk

Andrew Martin

Oxford University

Computing Laboratory

Wolfson Building, Parks Road, Oxford OX1 3QD, UK

E-mail: andrew.martin@comlab.ox.ac.uk

Library of Congress Control Number: 2009921804

CR Subject Classification (1998): D.4.6, K.6.5, E.3, C.2, C.3, D.2, H.4, H.5, K.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-00586-1 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-00586-2 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12634439 06/3180 5 4 3 2 1 0

Preface

This volume contains the 15 papers presented in the technical strand of the Trust 2009 conference, held in Oxford, UK in April 2009. Trust 2009 was the second international conference devoted to the technical and socio-economic aspects of trusted computing. The conference had two main strands, one devoted to technical aspects of trusted computing (addressed by these proceedings), and the other devoted to socio-economic aspects.

Trust 2009 built on the successful Trust 2008 conference, held in Villach, Austria in March 2008. The proceedings of Trust 2008, containing 14 papers, were published in volume 4968 of the *Lecture Notes in Computer Science* series.

The technical strand of Trust 2009 contained 15 original papers on the design and application of trusted computing. For these proceedings the papers have been divided into four main categories, namely:

- Implementation of trusted computing
- Attestation
- PKI for trusted computing
- Applications of trusted computing

The 15 papers included here were selected from a total of 33 submissions. 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.

We would also like to thank all the authors who submitted their papers to the technical strand of the Trust 2009 conference, all external referees, and all the attendees of the conference.

It is intended that this conference is the second in an annual series of conferences devoted to trusted computing, and we look forward to Trust 2010.

January 2009

Liqun Chen
Chris Mitchell

Organization

Trust 2009

The Second International Conference on Trusted Computing
(Technical Strand) was held at St. Hugh's College, Oxford, UK during
April 6–8, 2009

General Chair

Andrew Martin University of Oxford, UK

Program Chairs

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

Program Committee

Endre Bangerter	Bern University of Applied Sciences, Switzerland
David Challener	Lenovo, USA
James Davenport	University of Bath, UK
Robert Deng	Singapore Management University, Singapore
Loïc Duflot	SGDN/DCSSI, France
Paul England	Microsoft, USA
Sigrid Guergens	Fraunhofer, Germany
Dirk Kuhlmann	HP Laboratories, UK
Peter Lipp	IAIK, TU Graz, Austria
Javier Lopez	University of Malaga, Spain
Andrew Martin	University of Oxford, UK
Yi Mu	University of Wollongong, Australia
David Naccache	ENS, France
Heike Neumann	NXP Semiconductors, Germany
Elisabeth Oswald	University of Bristol, UK
Kenny Paterson	RHUL, UK
Raphael Phan	University of Loughborough, UK
Bart Preneel	KU Leuven, Belgium
Graeme Proudler	HP Laboratories, UK
Sihan Qing	Chinese Academy of Sciences, China
Carsten Rudolph	Fraunhofer, Germany
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany

VIII Organization

Jean-Pierre Seifert	Samsung Research, USA
Ari Singer	NTRU, USA
Sean Smith	Dartmouth College, USA
Christian Stüebe	Sirrix, Germany
Leendert van Doorn	AMD, USA
Vijay Varadharajan	Macquarie University, Australia

Steering Committee

Boris Balacheff	Hewlett-Packard Laboratories, UK
Ian Brown	University of Oxford, UK
Andrew Martin	University of Oxford, UK
Chris Mitchell	Royal Holloway, University of London, UK
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany

External Reviewers

Tien Tuan Anh Dinh	Sandra Marcello
Kurt Dietrich	Aybek Mukhamedov
Jim Grimmett	Aarthi Nagarajan
Xinyi Huang	Dan Page
Jun Ho Huh	Dries Schellekens
Qingguang Ji	Qingni Shen
Markulf Kohlweiss	Nigel Smart
Stephan Krenn	Ben Smyth
GaiCheng Li	Udaya Kiran Tupakula
Hans Löhr	Bogdan Warinschi
John Lyle	Marcel Winandy

Table of Contents

Implementation of Trusted Computing

Towards a Programmable TPM	1
<i>Paul England and Talha Tariq</i>	
ACPI: Design Principles and Concerns	14
<i>Loïc Dufлот, Olivier Levillain, and Benjamin Morin</i>	
Implementation Aspects of Mobile and Embedded Trusted Computing	29
<i>Kurt Dietrich and Johannes Winter</i>	
Modeling Trusted Computing Support in a Protection Profile for High Assurance Security Kernels	45
<i>Hans Löhr, Ahmad-Reza Sadeghi, Christian Stübле, Marion Weber, and Marcel Winandy</i>	

Attestation

Remote Attestation of Attribute Updates and Information Flows in a UCON System	63
<i>Mohammad Nauman, Masoom Alam, Xinwen Zhang, and Tamleek Ali</i>	
Measuring Semantic Integrity for Remote Attestation	81
<i>Fabrizio Baiardi, Diego Cilea, Daniele Sgandurra, and Francesco Ceccarelli</i>	

PKI for Trusted Computing

A PrivacyCA for Anonymity and Trust	101
<i>Martin Pirker, Ronald Toegl, Daniel Hein, and Peter Danner</i>	
Revocation of TPM Keys	120
<i>Stefan Katzenbeisser, Klaus Kursawe, and Frederic Stumpf</i>	

Applications I

Securing the Dissemination of Emergency Response Data with an Integrated Hardware-Software Architecture	133
<i>Timothy E. Levin, Jeffrey S. Dwoskin, Ganesha Bhaskara, Thuy D. Nguyen, Paul C. Clark, Ruby B. Lee, Cynthia E. Irvine, and Terry V. Benzal</i>	

Trustable Remote Verification of Web Services 153
John Lyle

Trustworthy Log Reconciliation for Distributed Virtual
Organisations 169
Jun Ho Huh and John Lyle

Attacking the BitLocker Boot Process 183
*Sven Törpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and
Jan Trukenmüller*

Applications II

Secure VPNs for Trusted Computing Environments 197
Steffen Schulz and Ahmad-Reza Sadeghi

Merx: Secure and Privacy Preserving Delegated Payments 217
Christopher Soghoian and Imad Aad

A Property-Dependent Agent Transfer Protocol 240
Eimear Gallery, Aarthi Nagarajan, and Vijay Varadharajan

Author Index 265