

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

Peter Lipp Ahmad-Reza Sadeghi
Klaus-Michael Koch (Eds.)

Trusted Computing – Challenges and Applications

First International Conference on Trusted Computing
and Trust in Information Technologies, TRUST 2008
Villach, Austria, March 11-12, 2008
Proceedings

Volume Editors

Peter Lipp
Graz University of Technology
Institute for Applied Information Processing
and Communications
Inffeldgasse 16a, 8010 Graz, Austria
E-mail: peter.lipp@iaik.tugraz.at

Ahmad-Reza Sadeghi
Ruhr-University Bochum
Chair for System Security
Universitätsstr. 150
44780 Bochum, Germany
E-mail: ahmad.sadeghi@trust.rub.de

Klaus-Michael Koch
Technikon Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
E-mail: koch@technikon.com

Library of Congress Control Number: 2008932592

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 3-540-68978-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68978-2 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 is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12279555 06/3180 5 4 3 2 1 0

Preface

This volume contains papers presented at TRUST 2008, the first international conference on Trusted Computing and Trust in Information Technologies, held in March 2008 in Villach, Austria. The aim of the conference was to create a joint scientific and networking platform covering the core issues of trust in IT systems and trusted computing and to bridge the gaps between international research groups and projects in closely related fields.

The organizers received 43 submissions from 17 countries. Each of the submitted papers was reviewed by three reviewers. Based on these reviews 13 papers were selected as suitable for the conference and the authors were asked to present their work. Further, six renowned speakers from academia, industry and the European Commission were invited for keynotes. The accepted papers are published in this volume together with one paper from Paul England, one of the invited speakers at TRUST 2008.

The conference was supported by the European Commission via the Open-TC project (FP6 IST-027635), by the Austrian Research Promotion Agency (FFG) and by the city of Villach.

We are very grateful to all the members of the Program Committee for their effort during the review process, to our invited speakers for their valuable talks, to all supporters, and the local organizers for making this conference the successful start of a hopefully long series of TRUST conferences!

March 2008

Peter Lipp
Ahmad-Reza Sadeghi

Organization

Scientific Chairs

Ahmad-Reza Sadeghi
Peter Lipp

Ruhr-University Bochum
Graz University of Technology

Organizer

Taru Kankkunen

WiTEC Austria (European Association for Women
in Science, Engineering and Technology)

Local Host

Klaus-Michael Koch

TECHNIKON Forschungs- und
Planungsgesellschaft mbH

Program Committee

Asokan, N.
Aura, Tuomas
Brandl, Hans
Breu, Ruth
England, Paul
Findeisen, Ralf
Grawrock, David
Härtig, Hermann
Haselsteiner, Ernst
Herzog, Peter
Katzenbeisser, Stefan
Kiayias, Aggelos
Kruegel, Christopher
Kuhlmann, Dirk
Lioy, Antonio
Martin, Andrew
Mitchell, Chris
Mao, Wenbo
Neumann, Heike
Paar, Christof
Persiano, Giuseppe
Preneel, Bart
Puccetti, Armand
Quisquater, Jean-Jacques

Nokia Research Center
Microsoft Research
Infineon Technologies AG
University of Innsbruck
Microsoft Research
AMD Saxony LLC & Co. KG
Intel
Dresden University of Technology
NXP Semiconductors
ISECOM
Philips Research
University of Connecticut
Vienna University of Technology
HP Labs Bristol
Politecnico di Torino
University of Oxford
Royal Holloway University of London
EMC Research China
NXP Semiconductors
Ruhr-University Bochum
University of Salerno
Katholieke Universiteit Leuven
Commissariat à l'Energie Atomique-LIST
Université Catholique de Louvain

VIII Organization

Rannenbergh, Kai
Rijmen, Vincent
Schunter, Matthias
Seifert, Jean-Pierre
Spitz, Stephan
Strongin, Geoffrey
Stüble, Christian
Thomborson, Clark
van Doorn, Leendert
Varadharajan, Vijay
Zhang, Xinwen

Goethe University of Frankfurt
Graz University of Technology
IBM Zurich
Samsung Research
Giesecke & Devrient
AMD
Sirrix AG, security technologies
University of Auckland
AMD
Macquarie University
Samsung Research

Keynotes

David Grawrock
Paul England
Martin Sadler
Ronald Perez
Bart Preneel
Dirk van Rooy

Intel
Microsoft
HP
IBM
Katholieke Universiteit Leuven
European Commission

Table of Contents

TRUST 2008

Practical Techniques for Operating System Attestation	1
<i>Paul England</i>	
TOCTOU, Traps, and Trusted Computing	14
<i>Sergey Bratus, Nihal D’Cunha, Evan Sparks, and Sean W. Smith</i>	
A Software-Based Trusted Platform Module Emulator	33
<i>Mario Strasser and Heiko Stamer</i>	
Towards Trust Services for Language-Based Virtual Machines for Grid Computing	48
<i>Tobias Vejda, Ronald Toegl, Martin Pirker, and Thomas Winkler</i>	
Embedded Trusted Computing with Authenticated Non-volatile Memory	60
<i>Dries Schellekens, Pim Tuyls, and Bart Preneel</i>	
The Zurich Trusted Information Channel – An Efficient Defence Against Man-in-the-Middle and Malicious Software Attacks	75
<i>Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, and Michael Baentsch</i>	
A Model for New Zealand’s Identity Verification Service	92
<i>Clark Thomborson</i>	
Pseudonymous Mobile Identity Architecture Based on Government-Supported PKI	107
<i>Konstantin Hyppönen, Marko Hassinen, and Elena Trichina</i>	
Para-Virtualized TPM Sharing	119
<i>Paul England and Jork Loeser</i>	
Slicing for Security of Code	133
<i>Benjamin Monate and Julien Signoles</i>	
Trusted Computing Serving an Anonymity Service	143
<i>Alexander Böttcher, Bernhard Kauer, and Hermann Härtig</i>	
Combining Biometric Authentication with Privacy-Enhancing Technologies	155
<i>Konstantin Hyppönen, Marko Hassinen, and Elena Trichina</i>	

A New Direct Anonymous Attestation Scheme from Bilinear Maps	166
<i>Ernie Brickell, Liqun Chen, and Jiangtao Li</i>	
On a Possible Privacy Flaw in Direct Anonymous Attestation (DAA) . . .	179
<i>Adrian Leung, Liqun Chen, and Chris J. Mitchell</i>	
Author Index	191