Lecture Notes in Computer Science 6101

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
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, 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

Alessandro Acquisti Sean W. Smith
Ahmad-Reza Sadeghi (Eds.)

Trust and Trustworthy Computing

Third International Conference, TRUST 2010
Berlin, Germany, June 21-23, 2010
Proceedings

Springer

Volume Editors

Alessandro Acquisti
Carnegie Mellon University, Heinz College
5000 Forbes Avenue, HBH 2105C, Pittsburgh, PA 15213, USA
E-mail: acquisti@andrew.cmu.edu

Sean W. Smith
Dartmouth College, Department of Computer Science
6211 Sudikoff Laboratory, Hanover, NH 03755-3510, USA
E-mail: sws@cs.dartmouth.edu

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

Library of Congress Control Number: 2010928338

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

ISSN 0302-9743
ISBN-10 3-642-13868-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13868-3 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 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the proceedings of the Third International Conference on Trust and Trustworthy Computing (TRUST), held at the Ritz-Carlton hotel in Berlin, Germany, June 21–23, 2010.

TRUST is a rapidly growing forum for research on the technical and socio-economic aspects of trustworthy infrastructures. TRUST provides an interdisciplinary forum for researchers, practitioners, and decision makers to explore new ideas and discuss experiences in building, designing, using, and understanding trustworthy computing systems.

The third edition of TRUST welcomed manuscripts in two different tracks: a Technical Strand and a Socio-economic Strand. We assembled an engaging program with 21 peer-reviewed technical papers and nine peer-reviewed socio-economic papers; eight keynotes from industry, academia, and government; and panel discussions on privacy and standards. In addition, this year, TRUST was co-located with four workshops: Trust in Cloud, Hardware Security, Emerging and Future Risks, and Anonymous Signatures.

We would like to thank numerous individuals for their effort and contribution to the conference and for making TRUST 2010 possible: the Organizing Committee members—Nadine Palacios and Marcel Winandy—for their tremendous help with all aspects of the organization; the Technical and Socio-economic Program Committee members, whose names are listed on the following pages, together with the names of external reviewers who helped us in the process of selecting manuscripts to be included in the conference proceedings; the keynote and invited speakers; and the invited panel speakers.

Finally, we express our gratitude to our sponsors, whose support was crucial to the success of TRUST 2010: Microsoft Research, Intel, Hewlett-Packard, TCG (Trusted Computing Group), Sirrix AG security technologies, Intrinsic ID, and CASED (Center for Advance Security Research Darmstadt).

June 2010

Alessandro Acquisti
Sean W. Smith
Ahmad-Reza Sadeghi

Organization

TRUST 2010

The Third International Conference on Trust and Trustworthy Computing was held at the Ritz-Carlton hotel in Berlin, Germany, June 21–23, 2010.

General Chair

Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany

Program Chairs

Technical Strand

Sean W. Smith	Dartmouth College, USA

Socio-economic Strand

Alessandro Acquisti	Carnegie Mellon University, USA

Organizing Committee

Nadine Palacios	Ruhr University Bochum, Germany
Marcel Winandy	Ruhr University Bochum, Germany

Program Committees

Technical Strand

N. Asokan	Nokia Research Center, Finland
Sergey Bratus	Dartmouth College, USA
Liqun Chen	HP Laboratories, UK
David Grawrock	Intel, USA
Cynthia Irvine	Naval Postgraduate School, USA
Bernhard Kauer	Technische Universität Dresden, Germany
Michael LeMay	University of Illinois Urbana-Champaign, USA
Michael Locasto	George Mason University, USA
Andrew Martin	University of Oxford, UK
Jon McCune	Carnegie Mellon University, USA
Chris Mitchell	Royal Holloway University, UK
David Naccache	ENS, France
Dimitris Pendarakis	IBM T.J. Watson Research Center, USA
Graeme Proudler	HP Laboratories, UK
Anand Rajan	Intel, USA
Scott Rotondo	Sun, USA

Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Radu Sion	Stony Brook University, USA
Sean W. Smith	Dartmouth College, USA
Christian Stüble	Sirrix, Germany
G. Edward Suh	Cornell University, USA
Leendert van Doorn	AMD, USA
Claire Vishik	Intel, UK

Socio-economic Strand

Alessandro Acquisti	Carnegie Mellon University, USA
Andrew A. Adams	Reading University, UK
Ian Brown	University of Oxford, UK
Johann Cas	Austrian Academy of Science, Austria
Lorrie Faith Cranor	Carnegie Mellon University, USA
Tamara Dinev	Florida Atlantic University, USA
Peter Gutmann	University of Auckland, New Zealand
Tristan Henderson	St Andrews University, UK
Adam Joinson	Bath University, UK
Eleni Kosta	Katholieke Universiteit Leuven, Belgium
Meryem Marzouki	French National Scientific Research Center (CNRS), France
Tyler Moore	Harvard University, USA
Deirdre Mulligan	UC Berkely, USA
Anne-Marie Oostveen	University of Oxford, UK
Andrew Patrick	Carleton University, Canada
Angela Sasse	University College London, UK
Jonathan Zittrain	Harvard University, USA

Steering Committee

Alessandro Acquisti	Carnegie Mellon University, USA
Boris Balacheff	Hewlett Packard, UK
Andrew Martin	University of Oxford, UK
Chris Mitchell	Royal Holloway University, UK
Sean Smith	Dartmouth College, USA
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Claire Vishik	Intel, UK

Additional Reviewers

Ellick Chan
Matthew Hicks
Hans Löhr
John Lyle
Cornelius Namiluko
Thomas Schneider
Ravinder Shankesi
Anna Shubina
Wattana Viriyasitavat
Christian Wachsmann
Marcel Winandy

Sponsors

Microsoft Research
Intel
Hewlett-Packard
TCG (Trusted Computing Group)
Sirrix AG security technologies
Intrinsic ID
CASED (Center for Advance Security Research Darmstadt)

Table of Contents

Technical Strand—Full Papers

Beyond Kernel-Level Integrity Measurement: Enabling Remote Attestation for the Android Platform 1
Mohammad Nauman, Sohail Khan, Xinwen Zhang, and Jean-Pierre Seifert

SBAP: Software-Based Attestation for Peripherals 16
Yanlin Li, Jonathan M. McCune, and Adrian Perrig

Key Attestation from Trusted Execution Environments 30
Kari Kostiainen, Alexandra Dmitrienko, Jan-Erik Ekberg, Ahmad-Reza Sadeghi, and N. Asokan

Anonymous Authentication with TLS and DAA 47
Emanuele Cesena, Hans Löhr, Gianluca Ramunno, Ahmad-Reza Sadeghi, and Davide Vernizzi

Group-Based Attestation: Enhancing Privacy and Management in Remote Attestation 63
Sami Alsouri, Özgür Dagdelen, and Stefan Katzenbeisser

Towards a Trusted Mobile Desktop 78
Marcel Selhorst, Christian Stüble, Florian Feldmann, and Utz Gnaida

Application of Trusted Computing in Automation to Prevent Product Piracy 95
Nora Lieberknecht

Lagrangian E-Voting: Verifiability on Demand and Strong Privacy 109
Łukasz Krzywiecki and Mirosław Kutyłowski

μTSS – A Simplified Trusted Software Stack 124
Christian Stüble and Anoosheh Zaerin

Requirements for an Integrity-Protected Hypervisor on the x86 Hardware Virtualized Architecture 141
Amit Vasudevan, Jonathan M. McCune, Ning Qu, Leendert van Doorn, and Adrian Perrig

A DAA Scheme Using Batch Proof and Verification 166
Liqun Chen

A Pairing-Based DAA Scheme Further Reducing TPM Resources 181
Ernie Brickell and Jiangtao Li

An Anonymous Attestation Scheme with Optional Traceability 196
Jiangtao Li and Anand Rajan

Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing 211
F. John Krautheim, Dhananjay S. Phatak, and Alan T. Sherman

SegSlice: Towards a New Class of Secure Programming Primitives for Trustworthy Platforms 228
Sergey Bratus, Michael E. Locasto, and Brian Schulte

Technical Strand—Short Papers

Escrowed Data and the Digital Envelope 246
King Ables and Mark D. Ryan

Engineering Attestable Services 257
John Lyle and Andrew Martin

Dynamic Enforcement of Platform Integrity 265
Martin Pirker, Ronald Toegl, and Michael Gissing

An Improved Memory Integrity Protection Scheme 273
Yin Hu and Berk Sunar

Robust Combiners for Software Hardening (Extended Abstract) 282
Amir Herzberg and Haya Shulman

The PUF Promise 290
Heike Busch, Miroslava Sotáková, Stefan Katzenbeisser, and Radu Sion

Socio-Economic Strand

Privacy Requirements Engineering for Trustworthy e-Government Services 298
Nikos Vrakas, Christos Kalloniatis, Aggeliki Tsohou, and Costas Lambrinoudakis

Can Competitive Insurers Improve Network Security? 308
Nikhil Shetty, Galina Schwartz, and Jean Walrand

Nudge: Intermediaries' Role in Interdependent Network Security 323
Jens Grossklags, Svetlana Radosavac, Alvaro A. Cárdenas, and John Chuang

How the Public Views Strategies Designed to Reduce the Threat of Botnets 337
Brent Rowe, Dallas Wood, and Douglas Reeves

Axiomatic and Behavioural Trust 352
Clark Thomborson

The Leap of Faith from Online to Offline: An Exploratory Study of Couchsurfing.org 367
Jun-E Tan

The Role of Soft Information in Trust Building: Evidence from Online Social Lending 381
Stefanie Pötzsch and Rainer Böhme

Software on the Witness Stand: What Should It Take for Us to Trust It? 396
Sergey Bratus, Ashlyn Lembree, and Anna Shubina

Workshop on Trust in the Cloud

Token-Based Cloud Computing: Secure Outsourcing of Data and Arbitrary Computations with Lower Latency 417
Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy

Workshop on Security Hardware

Oblivious Transfer Based on Physical Unclonable Functions (Extended Abstract) 430
Ulrich Rührmair

Author Index 441