Preface

This volume contains the proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST), held at Carnegie Mellon University, in Pittsburgh, Pennsylvania, USA, June 22–24, 2011.

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.

As in the previous edition, the fourth edition of TRUST welcomed manuscripts in two different strands: a technical strand and a socio-economic strand. We assembled an engaging program with 20 peer-reviewed technical papers and 3 peer-reviewed socio-economic papers; several keynotes from industry, academia, and government; and panel discussions. In addition, this year, TRUST was co-located with the Trusted Infrastructure Workshop (TIW), which is a 5-day Summer School in trustworthy computing.

We would like to thank numerous individuals for their effort and contribution to the conference and for making TRUST 2011 possible: the General Chairs Jonathan McCune (Carnegie Mellon University, USA) and Boris Balacheff (HP Labs, UK), as well as Marcel Winandy (Ruhr University Bochum, Germany) for their tremendous help with all aspects of the organization; the Technical and Socio-Economic Program Committees members, whose names are listed in the following pages and 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.

April 2011

Yolanta Beres
Adrian Perrig
Ahmad-Reza Sadeghi
Angela Sasse
TRUST 2011

The 4th International Conference on Trust and Trustworthy Computing was held at Carnegie Mellon University in Pittsburgh, PA, USA, June 22–24, 2011.

General Chairs

Jonathan McCune Carnegie Mellon University, USA
Boris Balacheff HP Labs, UK

Program Chairs

Technical Strand
Adrian Perrig Carnegie Mellon University, USA
Ahmad-Reza Sadeghi TU Darmstadt / Fraunhofer SIT, Germany

Socio-Economic Strand
Angela Sasse University College London, UK
Yolanta Beres HP Labs, UK

Program Committees

Technical Strand
Frederik Armknecht University of Mannheim, Germany
Marina Blanton University of Notre Dame, USA
Sergey Bratus Dartmouth College, USA
Christian Cachin IBM Research, Switzerland
Liqun Chen HP Laboratories, UK
Xuhua Ding Singapore Management University, Singapore
Paul England Microsoft, USA
Michael Franz University of California, Irvine, USA
Christian Gehrmann Swedish Institute of Computer Science, Sweden
David Grawrock Intel, USA
Helena Handschuh Intrinsic-ID, USA / KU Leuven, Belgium
Gernot Heiser NICTA, Australia
Thorsten Holz Ruhr University Bochum, Germany
Cynthia Irvine Naval Postgraduate School, USA
Stefan Katzenbeisser TU Darmstadt, Germany
VIII Organization

Michael LeMay University of Illinois Urbana-Champaign, USA
David Lie University of Toronto, Canada
Peter Lipp TU Graz, Austria
Michael Locasto University of Calgary, Canada
Andrew Martin University of Oxford, UK
Jon Millen The MITRE Corporation, USA
Chris Mitchell Royal Holloway, University of London, UK
David Naccache ENS, France
Dimitrios Pendarakis IBM Research, USA
Bart Preneel Katholieke Universiteit Leuven, Belgium
Graeme Proudler HP Laboratories, UK
Anand Rajan Intel Labs, USA
Scott Rotondo Oracle, USA
Mark Ryan University of Birmingham, UK
Jean-Pierre Seifert Technical University Berlin / T-Labs, Germany
Reiner Sailer IBM Research, USA
Matthias Schunter IBM Research, Switzerland
Sean Smith Dartmouth College, USA
Christian Stueble Sirrix, Germany
G. Edward Suh Cornell University, USA
Berk Sunar WPI, USA
Leendert van Doorn AMD, USA
Claire Vishik Intel, UK
Michael Waidner Fraunhofer SIT / TU Darmstadt, Germany
Marcel Winandy Ruhr University Bochum, Germany
Xinwen Zhang Huawei America Research Center, USA

Socio-Economic Strand

Alessandro Acquisti Carnegie Mellon University, USA
Andrew A. Adams Meiji University, Japan
Rainer Boehme University of Münster, Germany
Ian Brown University of Oxford, UK
Johann Cas Austrian Academy of Science
Tamara Dinev Florida Atlantic University, USA
Jens Grossklags Pennsylvania State University, USA
Peter Gutmann University of Auckland, New Zealand
Tristan Henderson University of St. Andrews, UK
Adam Joinson Bath University, UK
Eleni Kosta Katholieke Universiteit Leuven, Belgium
Meryem Marzouki French National Scientific Research Center
Tyler Moore Harvard University, USA
Andrew Patrick Office of the Privacy Commissioner of Canada
Jens Riegelsberger Google Research, UK
Steering Committee

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

Additional Reviewers

Luigi Catuogno Anbang Ruan
Hans Löhr Ludwig Seitz
John Lyle Anna Shubina
Emmanuel Owusu Dave Singelée
Alfredo Rial
## Table of Contents

### Session 1: Cloud and Virtualization

Verifying Trustworthiness of Virtual Appliances in Collaborative Environments ................................................... 1  
*Cornelius Namiluko, Jun Ho Huh, and Andrew Martin*

Towards a Trustworthy, Lightweight Cloud Computing Framework for Embedded Systems ................................. 16  
*Kurt Dietrich and Johannes Winter*

### Session 2: Physically Unclonable Functions

Side-Channel Analysis of PUFs and Fuzzy Extractors ................. 33  
*Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl*

Coalition Resistant Anonymous Broadcast Encryption Scheme Based on PUF ...................................................... 48  
*Lukasz Krzywiecki and Miroslaw Kutylowski*

A Practical Device Authentication Scheme Using SRAM PUFs ........ 63  
*Patrick Koeberl, Jiangtao Li, Anand Rajan, Claire Vishik, and Wei Wu*

### Session 3: Mobile Device Security

Practical Property-Based Attestation on Mobile Devices ............ 78  
*Kari Kostiainen, N. Asokan, and Jan-Erik Ekberg*

Taming Information-Stealing Smartphone Applications (on Android) ... 93  
*Tayin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W. Freeh*

Towards Permission-Based Attestation for the Android Platform  
(Short Paper) ................................................. 108  
*Ingo Bente, Gabi Drevo, Bastian Hellmann, Stephan Heuser, Joerg Vieweg, Josef von Helden, and Johannes Westhuis*

### Session 4: Socio-Economic Aspects of Trust

Trusting to Learn: Trust and Privacy Issues in Serious Games ....... 116  
*Miguel Malheiro, Charlene Jennett, Will Seager, and M. Angela Sasse*
Modifying Trust Dynamics through Cooperation and Defection in Evolving Social Networks ................................. 131  
Luca Allodi, Luca Chiodi, and Marco Cremonini

Who Is Concerned about What? A Study of American, Chinese and Indian Users’ Privacy Concerns on Social Network Sites (Short Paper) ................................................................. 146  
Yang Wang, Gregory Norcie, and Lorrie Faith Cranor

Session 5: Hardware Trust

Systematic Security Assessment at an Early Processor Design Stage . . . 154  
Ruirui Huang, David Grawrock, David C. Doughty, and G. Edward Suh

CPU Support for Secure Executables ........................................ 172  
Peter Williams and Rick Boivie

Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations .................................................. 188  
Pravin Prabhu, Ameen Akel, Laura M. Grupp, Wing-Kei S. Yu, G. Edward Suh, Edwin Kan, and Steven Swanson

Enforcing Executing-Implies-Verified with the Integrity-Aware Processor .......................................................... 202  
Michael LeMay and Carl A. Gunter

Session 6: Access Control

Home-Network Threats and Access Controls ................................. 217  
Mark Baugher and Victor Lortz

Contego: Capability-Based Access Control for Web Browsers (Short Paper) ........................................................ 231  
Tongbo Luo and Wenliang Du

Session 7: Privacy

Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information ................................................................. 239  
Emiliano De Cristofaro, Yanbin Lu, and Gene Tsudik

CertainLogic: A Logic for Modeling Trust and Uncertainty (Short Paper) .......................................................... 254  
Sebastian Ries, Sheikh Mahbub Habib, Max Mühlhäuser, and Vijay Varadharajan
Session 8: Trust Issues in Routing

AS-TRUST: A Trust Quantification Scheme for Autonomous Systems in BGP ................................................................. 262
   Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West,
   Sampath Kannan, Boon Thau Loo, Oleg Sokolsky, and Insup Lee

Incentivizing Responsible Networking via Introduction-Based Routing ................................................................. 277
   Gregory Frazier, Quang Duong, Michael P. Wellman, and Edward Petersen

Session 9: Crypto-Physical Protocols

Catching the Cuckoo: Verifying TPM Proximity Using a Quote Timing Side-Channel (Short Paper) ......................................................... 294
   Russell A. Fink, Alan T. Sherman, Alexander O. Mitchell, and David C. Challener

Group Distance Bounding Protocols (Short Paper) ...................... 302
   Srdjan Capkun, Karim El Defrawy, and Gene Tsudik

Author Index .............................................................................. 313