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 Stüeble 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 Löhre Bogdan Warinschi
John Lyle Marcel Winandy
# Table of Contents

**Implementation of Trusted Computing**

Towards a Programmable TPM ........................................... 1  
*Paul England and Talha Tariq*

ACPI: Design Principles and Concerns ................................. 14  
*Loïc Duflot, Olivier Levillain, and Benjamin Morin*

Implementation Aspects of Mobile and Embedded Trusted Computing .................................................. 29  
*Kurt Dietrich and Johannes Winter*

Modeling Trusted Computing Support in a Protection Profile for High Assurance Security Kernels ........................................... 45  
*Hans Löh, Ahmad-Reza Sadeghi, Christian Stüble, Marion Weber, and Marcel Winandy*

**Attestation**

Remote Attestation of Attribute Updates and Information Flows in a UCON System .................................................. 63  
*Mohammad Nauman, Masoom Alam, Xinwen Zhang, and Tamleek Ali*

Measuring Semantic Integrity for Remote Attestation ............... 81  
*Fabrizio Baiardi, Diego Cilea, Daniele Sgandurra, and Francesco Ceccarelli*

**PKI for Trusted Computing**

A PrivacyCA for Anonymity and Trust ..................................... 101  
*Martin Pirker, Ronald Toegl, Daniel Hein, and Peter Danner*

Revocation of TPM Keys .................................................. 120  
*Stefan Katzenbeisser, Klaus Kursawe, and Frederic Stumpf*

**Applications I**

Securing the Dissemination of Emergency Response Data with an Integrated Hardware-Software Architecture .................. 133  
*Timothy E. Levin, Jeffrey S. Dwoskin, Ganesha Bhaskara, Thuy D. Nguyen, Paul C. Clark, Ruby B. Lee, Cynthia E. Irvine, and Terry V. Benzel*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustable Remote Verification of Web Services</td>
<td>153</td>
</tr>
<tr>
<td><em>John Lyle</em></td>
<td></td>
</tr>
<tr>
<td>Trustworthy Log Reconciliation for Distributed Virtual Organisations</td>
<td>169</td>
</tr>
<tr>
<td><em>Jun Ho Huh and John Lyle</em></td>
<td></td>
</tr>
<tr>
<td>Attacking the BitLocker Boot Process</td>
<td>183</td>
</tr>
<tr>
<td><em>Sven Türpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmüller</em></td>
<td></td>
</tr>
</tbody>
</table>

**Applications II**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure VPNs for Trusted Computing Environments</td>
<td>197</td>
</tr>
<tr>
<td><em>Steffen Schulz and Ahmad-Reza Sadeghi</em></td>
<td></td>
</tr>
<tr>
<td>Merx: Secure and Privacy Preserving Delegated Payments</td>
<td>217</td>
</tr>
<tr>
<td><em>Christopher Soghoian and Imad Aad</em></td>
<td></td>
</tr>
<tr>
<td>A Property-Dependent Agent Transfer Protocol</td>
<td>240</td>
</tr>
<tr>
<td><em>Eimear Gallery, Aarthi Nagarajan, and Vijay Varadharajan</em></td>
<td></td>
</tr>
</tbody>
</table>

**Author Index**                                                                 | 265  |