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  Ruhr-University Bochum
Peter Lipp  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.  Nokia Research Center
Aura, Tuomas  Microsoft Research
Brandl, Hans  Infineon Technologies AG
Breu, Ruth  University of Innsbruck
England, Paul  Microsoft Research
Findeisen, Ralf  AMD Saxony LLC & Co. KG
Grawrock, David  Intel
Härtig, Hermann  Dresden University of Technology
Haselsteiner, Ernst  NXP Semiconductors
Herzog, Peter  ISECOM
Katzenbeisser, Stefan  Philips Research
Kiyias, Aggelos  University of Connecticut
Kruegel, Christopher  Vienna University of Technology
Kuhlmann, Dirk  HP Labs Bristol
Lioy, Antonio  Politecnico di Torino
Martin, Andrew  University of Oxford
Mitchell, Chris  Royal Holloway University of London
Mao, Wenbo  EMC Research China
Neumann, Heike  NXP Semiconductors
Paar, Christof  Ruhr-University Bochum
Persiano, Giuseppe  University of Salerno
Preneel, Bart  Katholieke Universiteit Leuven
Puccetti, Armand  Commissariat à l’Energie Atomique-LIST
Quisquater, Jean-Jacques  Università Catholique de Louvain
Rannenberg, 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
Paul England

TOCTOU, Traps, and Trusted Computing ........................................ 14
Sergey Bratus, Nihal D’Cunha, Evan Sparks, and Sean W. Smith

A Software-Based Trusted Platform Module Emulator ..................... 33
Mario Strasser and Heiko Stamer

Towards Trust Services for Language-Based Virtual Machines for Grid Computing ...................................................... 48
Tobias Vejda, Ronald Toegl, Martin Pirker, and Thomas Winkler

Embedded Trusted Computing with Authenticated Non-volatile Memory ................................................................. 60
Dries Scheltekens, Pim Tuyls, and Bart Preneel

The Zurich Trusted Information Channel – An Efficient Defence Against Man-in-the-Middle and Malicious Software Attacks .......... 75
Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, and Michael Baentsch

A Model for New Zealand’s Identity Verification Service .................. 92
Clark Thomborson

Pseudonymous Mobile Identity Architecture Based on Government-Supported PKI ......................................................... 107
Konstantin Hyppönen, Marko Hassinen, and Elena Trichina

Para-Virtualized TPM Sharing ...................................................... 119
Paul England and Jork Loeser

Slicing for Security of Code .......................................................... 133
Benjamin Monate and Julien Signoles

Trusted Computing Serving an Anonymity Service ....................... 143
Alexander Böttcher, Bernhard Kauer, and Hermann Härting

Combining Biometric Authentication with Privacy-Enhancing Technologies ............................................................... 155
Konstantin Hyppönen, Marko Hassinen, and Elena Trichina
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A New Direct Anonymous Attestation Scheme from Bilinear Maps</td>
<td>166</td>
</tr>
<tr>
<td><em>Ernie Brickell, Liqun Chen, and Jiangtao Li</em></td>
<td></td>
</tr>
<tr>
<td>On a Possible Privacy Flaw in Direct Anonymous Attestation (DAA)</td>
<td>179</td>
</tr>
<tr>
<td><em>Adrian Leung, Liqun Chen, and Chris J. Mitchell</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>191</td>
</tr>
</tbody>
</table>