

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

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

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Sokratis Katsikas Javier López
Günther Pernul (Eds.)

Trust, Privacy, and Security in Digital Business

Second International Conference, TrustBus 2005
Copenhagen, Denmark, August 22-26, 2005
Proceedings



Springer

Volume Editors

Sokratis Katsikas
University of the Aegean
Department of Information and Communication Systems Engineering
Karlovassi, 83200 Samos, Greece
E-mail: ska@aegean.gr

Javier López
University of Málaga
Departamento de Lenguajes y Ciencias de la Computación
Complejo Tecnológico, Campus de Teatinos, 29071 Málaga, Spain
E-mail: jlm@lcc.uma.es

Günther Pernul
University of Regensburg
Department of Information Systems
Universitätsstr. 31, 93053 Regensburg, Germany
E-mail: guenther.pernul@wiwi.uni-regensburg.de

Library of Congress Control Number: 2005930335

CR Subject Classification (1998): K.4.4, K.4, K.6, E.3, C.2, D.4.6, J.1

ISSN	0302-9743
ISBN-10	3-540-28224-6 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-28224-2 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11537878 06/3142 5 4 3 2 1 0

Preface

Sincerely welcome to the proceedings of the 2nd International Conference on Trust, Privacy, and Security in Digital Business, held in Copenhagen, Denmark, from August 22nd till 26th, 2005. This conference was the successor to the successful TrustBus 2004 conference, held in 2004 in conjunction with the DEXA conferences in Zaragoza. It was our goal that this event would be a forum to bring together researchers from academia and commercial developers from industry to discuss the state of the art of technology for establishing trust, privacy, and security in digital business. We thank the attendees for coming to Copenhagen to participate and debate the new emerging advances in this area.

The workshop program consisted of one invited talk and 11 regular technical paper sessions. The invited talk and keynote speech was delivered by Hannes Federrath from the Chair for Management of Information Security at the University of Regensburg, Germany, on “Privacy Enhanced Technology, Methods – Markets – Misuse”. A paper covering his talk is also contained in this book.

The regular paper sessions covered a broad range of topics, from access control issues to electronic auctioning, from trust and protocols to smart cards. The conference attracted over 100 submissions of which the Program Committee accepted 32 papers for presentation and inclusion in the conference proceedings. The authors of the accepted papers come from 16 different countries. The proceedings contain the revised versions of all accepted papers.

We would like to express our thanks to the people who helped put together the program: the Program Committee members and external reviewers for their timely and rigorous reviews of the papers; the DEXA Organizing Committee members in particular Mrs. Gabriela Wagner, for their help in administrative work; and, last but not least, Mr. Christian Schläger who was the main organizational force behind most of the involved tasks in making the conference possible.

Finally we would like to thank all authors who submitted papers, authors who presented papers, and the attendees who made this event an intellectually stimulating one. We hope they enjoyed the conference.

Athens, Màlaga, Regensburg
August 2005

Sokratis Katsikas
Javier López
Günther Pernul

Program Committee

General Chairperson

Sokratis Katsikas, University of the Aegean, Greece

Conference Program Chairpersons

Javier Lopez, University of Malaga, Spain

Guenther Pernul, University of Regensburg, Germany

Program Committee Members

Mike Burmester, Florida State University, USA

Marco Cassasa Mont, HP Labs, Bristol, UK

David W. Chadwick, University of Kent, UK

Elizabeth Chang, Curtin University of Technology, Australia

Frederic Cuppens, ENST Bretagne, France

Ernesto Damiani, University of Milan, Italy

Ed Dawson, Queensland University of Technology, Australia

Gurpreet Dhillon, VCU School of Business Richmond, USA

Tharam Dillon, University of Technology Sydney, Australia

Claudia Eckert, Technical University, Darmstadt, Germany

Hannes Federrath, University of Regensburg, Germany

Eduardo B. Fernandez, Florida Atlantic University, USA

Elena Ferrari, University of Insubria at Como, Italy

Simone Fischer-Huebner, Karlstad University, Sweden

Steven Furnell, University of Plymouth, UK

Juan M. González Nieto, Queensland University of Technology, Australia

Rüdiger Grimm, University of Technology Ilmenau, Germany

Dimitrios Gritzalis, Athens Univ. of Economics and Business, Greece

Stefanos Gritzalis, University of the Aegean, Greece

Ehud Gudes, Ben-Gurion University, Israel

Sigrid Gürgens, Fraunhofer SIT, Germany

Dipak Khakhar, Lund University, Sweden

Hiroaki Kikuchi, Tokai University, Japan

Klaus Kursawe, Katholieke Universiteit Leuven, Belgium

Costas Lambrinoudakis, University of the Aegean, Greece

Antonio Lioy, Politecnico di Torino, Italy

Diego Lopez, RedIRIS, Spain

Peter Lory, University of Regensburg, Germany

Olivier Markowitch, Université Libre de Bruxelles, Belgium

Fabio Martinelli, National Research Council - C.N.R. Pisa, Italy

Fabio Massacci, Università Degli Studi di Trento, Italy

Jose A. Montenegro, University of Malaga, Spain

Eiji Okamoto, University of Tsukuba, Japan

Martin Olivier, University of Pretoria, South Africa

Rolf Oppliger, eSECURITY Technologies, Switzerland

Ahmed Patel, University College, Dublin, Ireland
 Andreas Pfitzmann, University of Technology, Dresden, Germany
 Hartmut Pohl, University of Applied Sciences, Bonn-Rhein-Sieg, Germany
 Karl Posch, University of Technology, Graz, Austria
 Torsten Priebe, University of Regensburg, Germany
 Gerald Quirchmayr, University of Vienna, Austria
 Kai Rannenber, Goethe University Frankfurt, Germany
 Arnon Rosenthal, MITRE Corporation, USA
 Christoph Ruland, University of Siegen, Germany
 Germán Sáez, Universitat Politècnica de Catalunya, Spain
 Pierangela Samarati, University of Milan, Italy
 Matthias Schunter, IBM Zurich Research Lab, Switzerland
 Jose M. Sierra, Univ. Carlos III, Spain
 Mikko T. Siponen, University of Oulu, Finland
 Adrian Spalka, University of Bonn, Germany
 Leon Strous, De Nederlandsche Bank, Netherlands
 Stephanie Teufel, University of Fribourg, Switzerland
 Marianne Winslett, University of Illinois, USA
 Jianying Zhou, I2R, Singapore

External Reviewers

Andersson, Christer	Iliadis, John	Pisko, Evgenia
Balopoulos, Thodoris	Kalloniatis, Christos	Platis, Agapios
Bergmann, Mike	Kambourakis, George	Plössl, Klaus
Böhme, Rainer	Kantzavelou, Ioanna	Radmacher, Mike
Borcea, Katrin	Kim, Jintae	Rossnagel, Heiko
Boyd, Colin	Kokolakis, Spyros	Royer, Denis
Carminati, Barbara	Köpsell, Stefan	Schläger, Christian
Clauß, Sebastian	Kriegelstein, Thomas	Schlienger, Thomas
De Capitani di Vimercati, Sabrina	Lee, Adam	Soriano, Miquel
Dobmeier, Wolfgang	Lekkas, Dimitris	Squicciarini, Anna Cinzia
Dresp, Wiebke	Martucci, Leonardo	Steinbrecher, Sandra
Dritsas, Stelios	McManus, Leonie	Steinert, Martin
Erat, Andreas	Merten, Patrick	Svensson, Anders
Franz, Elke	Mitrou, Evangelia	van Le, Tri
Fritsch, Lothar	Mori, Paolo	Wendolsky, Rolf
Geneiatakis, Dimitris	Moussas, Vassilios	Westfeld, Andreas
Gilberg, Jörg	Munoz, Antonio	Wölfl, Thomas
González-Deleito, Nicolás	Muschall, Björn	Zhang, Charles
Herranz, Javier	Nowey, Thomas	
	Olson, Lars	
	Petrocchi, Marinella	

Table of Contents

Invited Talk

Privacy Enhanced Technologies: Methods – Markets – Misuse <i>Hannes Federrath</i>	1
--	---

Digital Business

Sec-Shield: Security Preserved Distributed Knowledge Management Between Autonomous Domains <i>Petros Belsis, Stefanos Gritzalis, Apostolos Malatras, Christos Skourlas, Ioannis Chalaris</i>	10
Protection Mechanisms Against Phishing Attacks <i>Klaus Plössl, Hannes Federrath, Thomas Nowey</i>	20
Dropout-Tolerant TTP-Free Mental Poker <i>Jordi Castellà-Roca, Francesc Sebé, Josep Domingo-Ferrer</i>	30
A Self-healing Mechanism for an Intrusion Tolerance System <i>Bumjoo Park, Kiejun Park, Sungsoo Kim</i>	41
Protecting Online Rating Systems from Unfair Ratings <i>Jianshu Weng, Chunyan Miao, Angela Goh</i>	50
Anonymous Payment in a Fair E-Commerce Protocol with Verifiable TTP <i>M. Magdalena Payeras-Capellà, Josep Lluís Ferrer-Gomila, Llorenç Huguet-Rotger</i>	60
Designing Secure E-Tendering Systems <i>Rong Du, Ernest Foo, Juan González Nieto, Colin Boyd</i>	70

Mobile/Wireless Services

A Multilateral Secure Payment System for Wireless LAN Hotspots <i>Stephan Groß, Sabine Lein, Sandra Steinbrecher</i>	80
Secure Group Communications over Combined Wired and Wireless Networks <i>Junghyun Nam, Seungjoo Kim, Dongho Won</i>	90

A Privacy Enhancement Mechanism for Location Based Service Architectures Using Transaction Pseudonyms <i>Oliver Jorns, Oliver Jung, Julia Gross, Sandford Bessler</i>	100
--	-----

Making Money with Mobile Qualified Electronic Signatures <i>Heiko Rossnagel, Denis Royer</i>	110
---	-----

Certificate Revocation/Index Search

Efficient Certificate Revocation System Implementation: Huffman Merkle Hash Tree (HuffMHT) <i>Jose L. Muñoz, Jordi Forné, Oscar Esparza, Manel Rey</i>	119
---	-----

Secure Index Search for Groups <i>Hyun-A Park, Jin Wook Byun, Dong Hoon Lee</i>	128
--	-----

Trust

Provision of Secure Policy Enforcement Between Small and Medium Governmental Organizations <i>Nikolaos Oikonomidis, Sergiu Tcaciuc, Christoph Ruland</i>	141
---	-----

Maximizing Utility of Mobile Agent Based E-Commerce Applications with Trust Enhanced Security <i>Ching Lin, Vijay Varadharajan, Yan Wang</i>	151
---	-----

The Fuzzy and Dynamic Nature of Trust <i>Elizabeth Chang, Patricia Thomson, Tharam Dillon, Farookh Hussain</i>	161
---	-----

Towards an Ontology of Trust <i>Lea Viljanen</i>	175
---	-----

Digital Signature

An Improved Group Signature Scheme <i>Jianhong Zhang, Jiancheng Zou, Yumin Wang</i>	185
--	-----

Efficient Member Revocation in Group Signature Schemes <i>Eun Young Choi, Hyun-Jeong Kim, Dong Hoon Lee</i>	195
--	-----

Conditional Digital Signatures <i>Marek Klonowski, Mirosław Kutylowski, Anna Lauks, Filip Zagórski</i>	206
---	-----

A Mediated Proxy Signature Scheme with Fast Revocation for Electronic Transactions <i>Seung-Hyun Seo, Kyung-Ah Shim, Sang-Ho Lee</i>	216
---	-----

Privacy

Privacy Enforcement for IT Governance in Enterprises: Doing It for Real <i>Marco Casassa Mont, Robert Thyne, Pete Bramhall</i>	226
An Adaptive Privacy Management System for Data Repositories <i>Marco Casassa Mont, Siani Pearson</i>	236
Privacy Preserving Data Mining Services on the Web <i>Ayça Azgın Hintoğlu, Yücel Saygın, Salima Benbernou, Mohand Said Hacid</i>	246
Reading Your Keystroke: Whose Mail Is It? <i>Sylvia Mercado Kierkegaard</i>	256

E-Auctions

A Novel Construction of Two-Party Private Bidding Protocols from Yao's Millionaires Problem <i>Huafei Zhu, Feng Bao</i>	266
An Improved Double Auction Protocol Against False Bids <i>JungHoon Ha, Jianying Zhou, SangJae Moon</i>	274
An Investigation of Dispute Resolution Mechanisms on Power and Trust: A Domain Study of Online Trust in e-Auctions <i>Glenn Bewsell, Rodger Jamieson, Adrian Gardiner, Deborah Bunker</i>	288

Smart Cards/Authentication

A Secure Fingerprint Authentication System on an Untrusted Computing Environment <i>Yonguha Chung, Daesung Moon, Taehae Kim, SungBum Pan</i>	299
Security Enhancement for Password Authentication Schemes with Smart Cards <i>Eun-Jun Yoon, Woo-Hun Kim, Kee-Young Yoo</i>	311

Securing Operating System Services Based on Smart Cards
 Luigi Catuogno, Roberto Gassirà, Michele Masullo, Ivan Visconti 321

Author Index 331