Lecture Notes in Computer Science 3184

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Sokratis Katsikas Javier Lopez
Günther Pernul (Eds.)

Trust and Privacy in Digital Business

First International Conference, TrustBus 2004
Zaragoza, Spain, August 30 - September 1, 2004
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 Lopez
University of Malaga, Computer Science Department
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: pernul@wiwi.uni-regensburg.de

Library of Congress Control Number: 2004110771

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

ISSN 0302-9743
ISBN 3-540-22919-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11312376 06/3142 5 4 3 2 1 0

Preface

Sincerely welcome to proceedings of the 1st International Conference on Trust and Privacy in Digital Business, Zaragoza, Spain, held from August 30th to September 1st, 2004. This conference was an outgrowth of the two successful TrustBus international workshops, held in 2002 and 2003 in conjunction with the DEXA conferences in Aix-en-Provence and in Prague. Being the first of a planned series of successful conferences it was our goal that this event would initiate 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 and privacy in digital business. We thank you all the attendees for coming to Zaragoza to participate and debate the new emerging advances in this area.

The conference program consisted of one invited talk and nine regular technical papers sessions. The invited talk and keynote speech was delivered by Ahmed Patel from the Computer Networks and Distributed Systems Research Group, University College Dublin, Ireland on "Developing Secure, Trusted and Auditable Services for E-Business: An Autonomic Computing Approach". 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 voting, from trust and protocols to digital rights management. The conference attracted close to 100 submissions of which the program committee accepted 29 papers for presentation and inclusion in the conference proceedings. The authors of the accepted papers come from 12 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, the DEXA organizing committee, in particular Mrs. Gabriela Wagner for her help in the 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, those who presented papers, and the attendees who made this event an intellectually stimulating one. We hope they enjoyed the conference.

Athens, Malaga, Regensburg
August 2004

Sokratis Katsikas
Javier Lopez
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
Peter Bramhall, HP Labs, Bristol, UK
Mike Burmester, Florida State University, USA
David W. Chadwick, University of Salford, UK
Frederic Cuppens, ENST Bretagne, France
Jorge Davila, Polytechnic Univ. of Madrid, Spain
Ed Dawson, Queensland University of Technology, Australia
Hannes Federrath, University of Regensburg, Germany
Eduardo B. Fernandez, Florida Atlantic University, USA
Elena Ferrari, University of Como, Italy
Simone Fischer-Huebner, Karlstad University, Sweden
Steven Furnell, University of Plymouth, UK
Rüdiger Grimm, University of Technology, Ilmenau, Germany
Stefanos Gritzalis, University of the Aegean, Greece
Dimitrios Gritzalis, Athens Univ. of Economics and Business, Greece
Ehud Gudes, Ben-Gurion University, Israel
Sigrid Guergens, Fraunhofer, Germany
Sushil Jajodia, George Mason University, USA
Kamal Karlapalem, IIIT Hyderabad, India
Dipak Khakhar, Lund University, Sweden
Hiroaki Kikuchi, Tokai University, Japan
Antonio Lioy, Politecnico di Torino, Italy
Diego Lopez, RedIRIS, Spain
Peter Lory, University of Regensburg, Germany
Masahiro Mambo, Tohoku University, Japan
Olivier Markowitch, Université Libre de Bruxelles, Belgium
Martin Olivier, University of Pretoria, South Africa
Eiji Okamoto, Universisty of Tsukuba, Japan
Rolf Oppliger, eSecurity Technologies, Switzerland
Ahmed Patel, University College Dublin, Ireland
Andreas Pfitzmann, University of Technology, Dresden, Germany
Birgit Pfitzmann, IBM Zurich Research Lab., Switzerland
Hartmut Pohl, FH Bonn-Rhein-Sieg, Germany
Karl Posch, University of Technology, Graz, Austria
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Gerald Quirchmayr, University of Vienna, Austria
Kai Rannenberg, University of Frankfurt, Germany

Arnon Rosenthal, MITRE Corporation, USA
Carsten Rudolph, Fraunhofer, Germany
Pierangela Samarati, University of Milan, Italy
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
Bhavani Thuraisingham, MITRE Corporation, USA
Ivan Visconti, ENS, France
Michael Waidner, IBM Zurich Research Lab., Switzerland
Marianne Winslett, University of Illinois, USA
Jianying Zhou, I2R, Singapore

External Reviewers

Angelis, George
Balopoulos, Thodoris
Bergmann, Mike
Boehme, Rainer
Bouabdallah, Ahmed
Boyd, Colin
Chen, Shiping
Clauss, Sebastian
D'Arco, Paolo
Erat, Andreas
Franz, Elke
Gilberg, Jörg
Guo, Huiping
Iliadis, John
Julisch, Klaus
Klimant, Herbert
Koepsell, Stefan
Kriegelstein, Thomas
Kühn, Ulrich
Lambrinoudakis, Costas
Martucci, Leonardo
Monahan, Brian
Muschall, Björn
Nikova, Svetla
Olson, Lars
Otenko, Sassa
Paul, Souradyuti
Pearson, Siani
Peng, Kun
Plank, Kilian
Priebe, Torsten
Proudler, Graeme
Rossnagel, Heiko
Rosulek, Mike
Roy, Sankardas
Schläger, Christian
Schlienger, Thomas
Schmidt, Nikita
Steinbrecher, Sandra
Steinert, Martin
Wang, Guilin
Westfeld, Andreas
Woelfl, Thomas
Yao, Chao
Zuccato, Albin

Table of Contents

Invited Talk

Developing Secure, Trusted and Auditable Services for e-Business: An Autonomic Computing Approach 1
Ahmed Patel

Trust

A Mechanism for Trust Sustainability Among Trusted Computing Platforms 11
Zheng Yan and Piotr Cofta

Enabling Trust-Awareness in Naming Services 20
Nicola Mezzetti

Virtual Trust in Distributed Systems 30
Semir Daskapan, Ana Cristina Costa, Willem G. Vree, and Amr A. Eldin

Modelling Trust Relationships in Distributed Environments 40
Weiliang Zhao, Vijay Varadharajan, and George Bryan

Access Control

Dynamically Changing Trust Structure in Capability Based Access Control Systems 50
Sandra Wortmann, Barbara Sprick, and Christoph Kobusch

On the Design of a New Trust Model for Mobile Agent Security 60
Ching Lin, Vijay Varadharajan, Yan Wang, and Yi Mu

e-Business Issues

Balancing Privacy and Trust in Electronic Marketplaces 70
Sandra Steinbrecher

Reducing Server Trust in Private Proxy Auctions 80
Giovanni Di Crescenzo, Javier Herranz, and Germán Sáez

Secure Ad-Hoc mBusiness: Enhancing WindowsCE Security 90
Florina Alménarez, Daniel Díaz, and Andrés Marín

Role-Based Privilege Management Using Attribute Certificates and Delegation . . 100
Gail-Joon Ahn, Dongwan Shin, and Longhua Zhang

Privacy

Consent as a Threat. A Critical Approach to Privacy Negotiation in e-Commerce Practices 110
A. Daniel Oliver-Lalana

Dealing with Privacy Obligations: Important Aspects and Technical Approaches . 120
Marco Casassa Mont

Offer Privacy in Mobile Agents Using Conditionally Anonymous Digital Signatures 132
Ming Yao, Matt Henricksen, Ernest Foo, and Ed Dawson

Privacy Preserving Data Generation for Database Application Performance Testing 142
Yongge Wang, Xintao Wu, and Yuliang Zheng

e-Voting

An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness 152
Riza Aditya, Byoungcheon Lee, Colin Boyd, and Ed Dawson

Trust in Public Administration e-Transactions: e-Voting in the UK 162
Alexandros Xenakis and Ann Macintosh

Protocols

An Unbalanced Protocol for Group Key Exchange 172
Javier Herranz and Jorge L. Villar

Certified E-Mail with Temporal Authentication: An Improved Optimistic Protocol 181
Clemente Galdi and Raffaella Giordano

Efficient Password-Based Group Key Exchange 191
Su Mi Lee, Jung Yeon Hwang, and Dong Hoon Lee

Optimality in Asynchronous Contract Signing Protocols 200
Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, and Llorenç Huguet-Rotger

Copyright Protection

Development of Visible Anti-copy Patterns 209
JongWeon Kim, KyuTae Kim, JungSoo Lee, and JongUk Choi

Holographic Image Watermarking for Secure Content 219
KyuTae Kim, JongWeon Kim, JungSoo Lee, and JongUk Choi

Hybrid Fingerprint Matching on Programmable Smart Cards 232
Tommaso Cucinotta, Riccardo Brigo, and Marco Di Natale

Protecting ASF Movie on VOD 242
Ji-Hyun Park, Jeong-Hyun Kim, and Ki-Song Yoon

Multicast

DiffSig: Differentiated Digital Signature for Real-Time Multicast Packet Flows . . 251
Namhi Kang and Christoph Ruland

Large-Scale Pay-As-You-Watch for Unicast and Multicast Communications 261
Antoni Martínez-Ballesté, Francesc Sebé, and Josep Domingo-Ferrer

PKI, Signature Schemes

Reducing the Communication Overhead of an Offline Revocation Dictionary 269
Jose L. Muñoz, Jordi Forné, Oscar Esparza, Josep Pegueroles, and Esteve Pallarès

Breaking Down Architectural Gaps in Smart-Card Middleware Design 279
Tommaso Cucinotta, Marco Di Natale, and David Corcoran

On the Security of the Lee-Hwang Group-Oriented Undeniable Signature Schemes 289
Guilin Wang, Jianying Zhou, and Robert H. Deng

Author Index 299