

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Simone Fischer-Hübner  
Sokratis Katsikas Gerald Quirchmayr (Eds.)

# Trust, Privacy and Security in Digital Business

9th International Conference, TrustBus 2012  
Vienna, Austria, September 3-7, 2012  
Proceedings

## Volume Editors

Simone Fischer-Hübner

Karlstad University, Department of Computer Science

Universitetsgatan 2, 65188, Karlstad, Sweden

E-mail: simone.fischer-huebner@kau.se

Sokratis Katsikas

University of Piraeus, Department of Digital Systems

150 Androutsou St., 18532 Piraeus, Greece

E-mail: ska@unipi.gr

Gerald Quirchmayr

University of Vienna, Research Group Multimedia Information Systems

Liebiggasse 4, 1010 Wien, Austria

E-mail: gerald.quirchmayr@univie.ac.at

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-32286-0

e-ISBN 978-3-642-32287-7

DOI 10.1007/978-3-642-32287-7

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012943036

CR Subject Classification (1998): D.4.6, K.6.5, E.3, K.4.4, H.2.7, C.2, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

The advances in information and communication technologies have raised new opportunities for the implementation of novel applications and the provision of high-quality services over global networks. The aim is to utilize this “information society era” to improve the quality of life for all citizens, disseminating knowledge, strengthening social cohesion, generating earnings, and finally ensuring that organizations and public bodies remain competitive in the global electronic marketplace. Unfortunately, such a rapid technological evolution cannot be problem-free. Concerns are raised regarding the “lack of trust” in electronic procedures and the extent to which information security and user privacy can be ensured.

In answer to these concerns, the 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012) was held in Vienna during September 4–6, 2012. TrustBus 2012 brought together researchers from different disciplines, developers, and users, all interested in the critical success factors of digital business systems, and provided an international forum for researchers and practitioners to exchange information regarding advancements in the state of the art and practice of trust and privacy in digital business.

TrustBus 2012 received 42 paper submissions, which were all reviewed by at least two, and most of them by three or four members of the international Program Committee (PC). Based on the reviews and discussions between PC Chairs and PC members, 16 full papers and three short papers were finally accepted for presentation at the conference. Topics addressed by the accepted papers published in the proceedings include Web security, secure management processes and procedures, access control, trust models, privacy policies and privacy-enhancing technologies, cryptographic solutions as well as secure services, databases, and data warehouses. An invited keynote talk was given by Sarah Spiekermann, Vienna University of Economics and Business, on “Privacy - A New Era?”. Furthermore, TrustBus organized in 2012 for the first time a special session, in which EU FP7 research projects related to trust, privacy, and security presented their recent research results.

We would like to thank all authors, especially those who presented their work selected for the program, as well as all EU project presenters. Moreover, we are very grateful to all PC members and additional reviewers who contributed with thorough reviews and participated in PC discussions ensuring a high quality of all accepted papers. We also owe special thanks to Sarah Spiekermann for contributing with her keynote talk.

Last but not least, we gratefully acknowledge the valuable help by Costas Lambrinoudakis when preparing TrustBus 2012 and by the local DEXA organizer Gabriela Wagner for her outstanding support.

June 2012

Simone Fischer-Hübner  
Sokratis Katsikas  
Gerald Quirchmayr

# Organization

## General Chair

Quirchmayr, Gerald

University of Vienna, Austria

## Program Committee Co-chairs

Fischer-Hübner, Simone  
Katsikas, Sokratis

Karlstad University, Sweden  
University of Piraeus, Greece

## Program Committee

Acquisti, Alessandro  
Agudo, Isaac  
Casassa Mont, Marco  
Chadwick, David  
Chu, Cheng-Kang  
Clarke, Nathan  
Cuppens, Frederic  
De Capitani di Vimercati,  
    Sabrina  
Eloff, Jan  
Fernandez, Eduardo B.  
Fernandez-Gago, Carmen  
Foresti, Sara  
Furnell, Steven  
Fuss, Juergen

Carnegie Mellon University, USA  
University of Malaga, Spain  
HP Labs Bristol, UK  
University of Kent, UK  
I2R, Singapore  
Plymouth University, UK  
ENST Bretagne, France

Geneiatakis, Dimitris  
Gonzalez-Nieto, Juan M.  
Gritzalis, Dimitris

University of Milan, Italy  
University of Pretoria, South Africa  
Florida Atlantic University, USA  
University of Malaga, Spain  
University of Milan, Italy  
Plymouth University, UK  
University of Applied Science in Hagenberg,  
    Austria  
University of Piraeus, Greece  
Queensland University of Technology, Australia  
Athens University of Economics and Business,  
    Greece

Gritzalis, Stefanos  
Hansen, Marit

University of the Aegean, Greece  
Independent Center for Privacy Protection,  
    Germany

Jøsang, Audun  
Kalloniatis, Christos  
Karyda, Maria  
Kesdogan, Dogan  
Kokolakis, Spyros  
Lambrinoudakis, Costas

Oslo University, Norway  
University of the Aegean, Greece  
University of the Aegean, Greece  
University of Siegen, Germany  
University of the Aegean, Greece  
University of Piraeus, Greece

Lioy, Antonio	Politecnico di Torino, Italy
Lopez, Javier	University of Malaga, Spain
Markowitch, Olivier	Université Libre de Bruxelles, Belgium
Martinelli, Fabio	CNR, Italy
Matyas, Vashek	Masaryk University, Czech Republic
Mitchell, Chris	Royal Holloway, University of London, UK
Mouratidis, Haris	University of East London, UK
Rajarajan, Muttukrishnan	City University, UK
Okamoto, Eiji	University of Tsukuba, Japan
Olivier, Martin S.	University of Pretoria, South Africa
Oppliger, Rolf	eSecurity Technologies, Switzerland
Papadaki, Maria	Plymouth University, UK
Pashalidis, Andreas	Katholieke Universiteit Leuven, Belgium
Patel, Ahmed	Kingston University (UK) - University Kebangsaan, Malaysia
Pernul, Günther	University of Regensburg, Germany
Posegga, Joachim	University of Passau, Germany
Rannenber, Kai	Goethe University of Frankfurt, Germany
Rizomiliotis, Panagiotis	University of the Aegean, Greece
Rudolph, Carsten	Fraunhofer Institute for Secure Information Technology, Germany
Ruland, Christoph	University of Siegen, Germany
Samarati, Pierangela	University of Milan, Italy
Schaumueller-Bichl, Ingrid	University of Applied Science in Hagenberg, Austria
Schunter, Matthias	Intel Labs, Germany
Soriano, Miguel	UPC, Spain
Theoharidou, Marianthi	Athens University of Economics and Business, Greece
Tsochou, Aggeliki	University of Piraeus, Greece
Teufel, Stephanie	University of Fribourg, Switzerland
Tjoa, A Min	Technical University of Vienna, Austria
Tomlinson, Allan	Royal Holloway, University of London, UK
Weipl, Edgar	SBA, Austria
Xenakis, Christos	University of Piraeus, Greece

# Table of Contents

## Web Security

How Much Network Security Must Be Visible in Web Browsers? . . . . .	1
<i>Tobias Hirsch, Luigi Lo Iacono, and Ina Wechsung</i>	
A User-Level Authentication Scheme to Mitigate Web Session-Based Vulnerabilities . . . . .	17
<i>Bastian Braun, Stefan Kucher, Martin Johns, and Joachim Posegga</i>	
Access Control Configuration for J2EE Web Applications: A Formal Perspective (Short Paper) . . . . .	30
<i>Matteo Maria Casalino, Romuald Thion, and Mohand-Said Hacid</i>	

## Secure Management Processes and Procedures

Cloud Separation: Stuck Inside the Cloud . . . . .	36
<i>Waldo Delpont and Martin S. Olivier</i>	
Proposed Control Procedure to Mitigate the Risks of Strategic Information Outflow in the Recruitment Process . . . . .	50
<i>Kashif Syed, Pavol Zavorsky, Dale Lindskog, Ron Ruhl, and Shaun Aghili</i>	

## Access Control

An Autonomous Social Web Privacy Infrastructure with Context-Aware Access Control . . . . .	65
<i>Michael Netter, Sabri Hassan, and Günther Pernul</i>	
A Prototype for Enforcing Usage Control Policies Based on XACML . . .	79
<i>Aliaksandr Lazouski, Fabio Martinelli, and Paolo Mori</i>	

## Intrusion Detection - Trust

A Conceptual Framework for Trust Models . . . . .	93
<i>Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez</i>	
Advances and Challenges in Standalone Host-Based Intrusion Detection Systems . . . . .	105
<i>Vit Bukac, Pavel Tucek, and Martin Deutsch</i>	



## Applied Cryptography

Encrypted Adaptive Storage Model – Analysis and Performance Tests .....	118
<i>Marcin Gorawski, Michal Lorek, and Michal Gorawski</i>	
Efficient Comparison of Encrypted Biometric Templates .....	129
<i>Michael Dorn, Peter Wackersreuther, and Christian Böhm</i>	
Short and Efficient Identity-Based Undeniable Signature Scheme (Short Paper) .....	143
<i>Rouzbeh Behnia, Swee-Huay Heng, and Che-Sheng Gan</i>	

## Privacy

Damage Sharing May Not Be Enough: An Analysis of an Ex-ante Regulation Policy for Data Breaches .....	149
<i>Giuseppe D'Acquisto, Marta Flamini, and Maurizio Naldi</i>	
Flexible Regulation with Privacy Points (Short Paper) .....	161
<i>Hanno Langweg and Lisa Rajbhandari</i>	

## Secure Services, Databases and Data Warehouses

On the Security of the Non-Repudiation of Forwarding Service .....	167
<i>Rainer Schick and Christoph Ruland</i>	
Profitability and Cost Management of Trustworthy Composite Services .....	179
<i>Hisain Elshaafi, Jimmy McGibney, and Dmitri Botvich</i>	
Query Auditing for Protecting Max/Min Values of Sensitive Attributes in Statistical Databases .....	192
<i>Ta Vinh Thong and Levente Buttyán</i>	
Verification of Security Coherence in Data Warehouse Designs (Short Paper) .....	207
<i>Ali Salem, Salah Triki, Hanène Ben-Abdallah, Nouria Harbi, and Omar Boussaid</i>	

## Presentation of EU Projects (Extended Abstracts)

Towards the Secure Provision and Consumption in the Internet of Services .....	214
<i>Luca Viganò</i>	
WebSand: Server-Driven Outbound Web-Application Sandboxing .....	216
<i>Martin Johns and Joachim Posegga</i>	

Attribute-Based Credentials for Trust (ABC4Trust) . . . . .	218
<i>Ahmad Sabouri, Ioannis Krontiris, and Kai Rannenberg</i>	
uTRUSTit – Usable Trust in the Internet of Things . . . . .	220
<i>Christina Hochleitner, Cornelia Graf, Peter Wolkerstorfer, and Manfred Tscheligi</i>	
Challenges for Advanced Security Monitoring – The MASSIF Project . . .	222
<i>Roland Rieke, Elsa Prieto, Rodrigo Diaz, Hervé Debar, and Andrew Hutchison</i>	
Decentralized, Cooperative, Secure and Privacy – Aware Monitoring for Trustworthiness . . . . .	224
<i>DEMONS Project Consortium</i>	
PASSIVE: Policy-Assessed System-Level Security of Sensitive Information Processing in Virtualised Environments . . . . .	227
<i>Panagiotis Rizomiliotis and Charalambos Skianis</i>	
Policy and Security Configuration Management . . . . .	229
<i>Henrik Plate</i>	
Challenges and Current Results of the TWISNet FP7 Project . . . . .	232
<i>Markus Wehner, Sven Zeisberg, Nouha Oualha, Alexis Olivereau, Mike Ludwig, Dan Tudose, Laura Gheorghe, Emil Slusanschi, Basil Hess, Felix von Reischach, and David Bateman</i>	
Aniketos: Challenges and Results . . . . .	234
<i>Miguel Ponce de Leon, Richard Sanders, Per Håkon Meland, Marina Egea, and Zeta Dooly</i>	
Ubiquitous Participation Platform for POLicy Making (UbiPOL): Security and Identity Management Considerations . . . . .	236
<i>Aggeliki Tsohou, Habin Lee, Yacine Rebahi, Mateusz Khalil, and Simon Hohberg</i>	
Secure Embedded Platform with Advanced Process Isolation and Anonymity Capabilities . . . . .	238
<i>Marc-Michael Bergfeld, Holger Bock, Roderick Bloem, Jan Blonk, Gregory Conti, Kurt Dietrich, Matthias Junk, Florian Schreiner, Stephan Spitz, and Johannes Winter</i>	
<b>Author Index . . . . .</b>	<b>241</b>