IFIP Advances in Information and Communication Technology 396

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

> *IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is about information processing may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Simone Fischer-Hübner
Elisabeth de Leeuw Chris Mitchell (Eds.)

Policies and Research in Identity Management

Third IFIP WG 11.6 Working Conference, IDMAN 2013
London, UK, April 8-9, 2013
Proceedings

Springer

Volume Editors

Simone Fischer-Hübner
Karlstad University, Department of Computer Science
Universitetsgatan 1, 65188 Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Elisabeth de Leeuw
IDTOPIQ - Security & Identity Management
Pracanalaan 80, 1060 RC Amsterdam, The Netherlands
E-mail: elisabeth.de.leeuw@xs4all.nl

Chris Mitchell
University of London, Information Security Group
Royal Holloway, Egham, Surrey TW20 0EX, UK
E-mail: me@chrismitchell.net

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-37281-0 e-ISBN 978-3-642-37282-7
DOI 10.1007/978-3-642-37282-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013933703

CR Subject Classification (1998): K.6.5, C.3, D.4.6, E.3, J.1

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

This volume contains the papers presented at IFIP IDMAN 2013: the Third IFIP WG 11.6 Working Conference on Policies and Research in Identity Management held during April, 8–9, 2013, at Royal Holloway, University of London, UK. Building on the success of IDMAN 2007 and 2010 (which were held in Rotterdam and Oslo, respectively), this conference focused on the theory, technologies, and applications of identity management.

The world of the twenty-first st century is, more than ever, global and impersonal. As a result of increasing cyber fraud and cyber terrorism, the demand for better technical methods of identification is growing, not only in companies and organizations but also in the world at large. Moreover, in our society digital identities increasingly play a role in the provision of eGovernment and eCommerce services. For practical reasons, identity management systems are needed that are usable and interoperable. At the same time, individuals increasingly leave trails of personal data when using the Internet, which allow them to be profiled and which may be stored for many years to come. Technical trends such as cloud computing and pervasive computing make personal data processing non-transparent, and make it increasingly difficult for users to control their personal spheres. As part of this tendency, surveillance and monitoring are increasingly present in society, both in the public and private domains. While the original intention is to contribute to security and safety, surveillance and monitoring might, in some cases, have unintended or even contradictory effects. Moreover, the omnipresence of surveillance and monitoring systems might directly conflict with public and democratic liberties. These developments raise substantial new challenges for privacy and identity management at the technical, social, ethical, regulatory, and legal levels. Identity management challenges the information security research community to focus on interdisciplinary and holistic approaches, while retaining the benefits of previous research efforts.

Papers offering research contributions to the area of identity management were solicited for submission to the Third IFIP WG 11.6 IDMAN conference. There were 26 submissions to IFIP IDMAN 2013. Each submission was reviewed by at least three Program Committee members. The Program Committee decided to accept six full and four short "work in progress" papers. The program also included two invited talks by Angela Sasse, University College London, and Bart Jacobs, Radboud University Nijmegen, as well as a panel on "Risk Analysis Approaches for Identity Management Systems" organized in cooperation with the Norwegian PETweb II project. IFIP IDMAN 2013 was also collocated with a workshop organized by the EPSRC-funded Future of Identity Network of Excellence, which took place immediately after the end of conference. These proceedings include the accepted full and short papers, the keynote paper by Bart Jacobs, as well as short position papers by the panelists.

We would like to thank all authors, especially those who presented their work selected for the program. Moreover, we are very grateful to all PC members and additional reviewers, who contributed with thorough reviews and participated in the PC discussions. We owe special thanks to David Chadwick and Jozef Vyskoc, who volunteered to shepherd some of the accepted papers.

We gratefully acknowledge the contributions of the Organizing Committee Chairs Haitham Al-Sinani and Marcelo Carlomagno Carlos. We also thank the EasyChair conference system provider for granting us free access to their excellent conference management system. Last but not least, we would like to thank all sponsors for their generous support.

January 2013

Simone Fischer-Hübner
Elisabeth de Leeuw
Chris Mitchell

Organization

Conference General Chair

Chris Mitchell	Royal Holloway, University of London, UK

Programme Committee Co-chairs

Simone Fischer-Hübner	Karlstad University, Sweden, IFIP WG 11.6 chair
Elisabeth de Leeuw	The Netherlands

Local Organizing Committee Chair

Haitham Al-Sinani	Royal Holloway, University of London, UK
Marcelo Carlomagno Carlos	Royal Holloway, University of London, UK

Program Committee

Haitham Al-Sinani	Royal Holloway, University of London, UK
Claudio Agostino Ardagna	Università degli Studi di Milano, Italy
Alessandro Armando	DIST - University of Genova, Italy
Bharat Bhargava	Purdue University, USA
Sonja Buchegger	Royal Institute of Technology (KTH), Sweden
David Chadwick	University of Kent, UK
Elisabeth De Leeuw	IdTopIQ, The Netherlands
Simone Fischer-Hübner	Karlstad University, Sweden
Sara Foresti	Università degli Studi di Milano, Italy
Lothar Fritsch	Norwegian Computing Center, Norway
Steven Furnell	University of Plymouth, UK
Stefanos Gritzalis	University of the Aegean, Greece
Thomas Gross	University of Newcastle upon Tyne, UK
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany
Hans Hedbom	Karlstad University, Sweden
Alejandro Hevia	University of Chile, Chile
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Bart Jacobs	Radboud University Nijmegen, The Netherlands

Lech Janczewski	The University of Auckland, New Zealand
Ronald Leenes	Tilburg University, The Netherlands
Javier Lopez	University of Malaga, Spain
Chris Mitchell	Royal Holloway, University of London, UK
Andreas Pashalidis	K.U. Leuven, Belgium
Aljosa Pasic	Atos Origin, Spain
Siani Pearson	HP Labs, UK
Günther Pernul	Universität Regensburg, Germany
Geraint Price	Royal Holloway, University of London, UK
Muttukrishnan Rajarajan	City University London, UK
Kai Rannenberg	Goethe University Frankfurt, Germany
Einar Snekkenes	Gjövik University College, Norway
Rama Subramaniam	Valiant Technologies, India
Pedro Veiga	FCCN, Portugal
Jozef Vyskoc	VaF, Slovakia
Rose-Mharie Åhlfeldt	University of Skövde, Sweden

Additional Reviewers

Bodriagov, Oleksandr	Kreitz, Gunnar
Broser, Christian	Mitrou, Lilian
Carbone, Roberto	Ranise, Silvio
Deuker, Andre	Reisser, Andreas
Drogkaris, Prokopios	Rodríguez Cano, Guillermo
Greschbach, Benjamin	Sabouri, Ahmad
Hassan, Sabri	Veseli, Fatbardh

Table of Contents

Keynote paper

Towards Practical Attribute-Based Identity Management: The IRMA Trajectory 1
Gergely Alpár and Bart Jacobs

Session 1 - Privacy and Identity Management

Data Protection by Default in Identity-Related Applications 4
Marit Hansen

Privacy-Friendly Checking of Remote Token Blacklists 18
Roel Peeters and Andreas Pashalidis

Session 2 - Anonymous Credentials

Concepts and Languages for Privacy-Preserving Attribute-Based Authentication 34
Jan Camenisch, Maria Dubovitskaya, Anja Lehmann, Gregory Neven, Christian Paquin, and Franz-Stefan Preiss

Efficient Selective Disclosure on Smart Cards Using Idemix 53
Pim Vullers and Gergely Alpár

Session 3 - Authentication and Access Control

Identity Management and Integrity Protection in Publish-Subscribe Systems 68
Anders Fongen and Federico Mancini

Extended HTTP Digest Access Authentication 83
Henning Klevjer, Kent Are Varmedal, and Audun Jøsang

Panel Session – Risk Management of Identity Management

Executable Model-Based Risk Assessment Method for Identity Management Systems (Position Paper) 97
Ebenezer Paintsil and Lothar Fritsch

Privacy Risk Analysis is about Understanding Conflicting Incentives (Position Paper) 100
Einar Snekkenes

Risk Analysis of Identity Management Approaches Employing Privacy Protection Goals (Position Paper) 104
Marit Hansen

Session 4 - Identity Management with Smart Cards

The Radboud Reader: A Minimal Trusted Smartcard Reader for Securing Online Transactions 107
Erik Poll and Joeri de Ruiter

Extending EMV Payment Smart Cards with Biometric On-Card Verification 121
Olaf Henniger and Dimitar Nikolov

Session 5 - Federated Identity Management

Dynamic Identity Federation Using Security Assertion Markup Language (SAML) 131
Md. Sadek Ferdous and Ron Poet

Logout in Single Sign-on Systems 147
Sanna Suoranta, Asko Tontti, Joonas Ruuskanen, and Tuomas Aura

Author Index 161