Privacy and Identity Management for Life

Jan Camenisch • Simone Fischer-Hübner
Kai Rannenberg
Editors

Privacy and Identity Mangement for Life

Springer

Editors
Jan Camenisch
IBM Research - Zürich
Säumerstrasse 4
8803 Rüschlikon
Switzerland
jca@zurich.ibm.com

Simone Fischer-Hübner
Universitetsgatan 2
65188 Karlstad
Sweden
simone.fischer-huebner@kau.se

Kai Rannenberg
Goethe University Frankfurt
T-Mobile Chair of Mobile Business & Multilateral Security
Grueneburgplatz 1
60629 Frankfurt/Main
Germany
Kai.Rannenberg@m-chair.net
www.m-chair.net

ISBN 978-3-642-20316-9 e-ISBN 978-3-642-20317-6
DOI 10.1007/978-3-642-20317-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011930188

Cover design: deblik, Berlin

Printed on acid-free paper

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

To the memory of our colleague and friend Andreas Pfitzmann

The protection of people's privacy was dear to Andreas' heart. He was an inspiration to all of us, and many of the results presented in this book owe to him.

Preface

Publication is a self-invasion of privacy.

Marshall McLuhan

Individuals in the Information Society want to safeguard their autonomy and retain control over their personal information, irrespective of their activities. Information technologies generally do not consider those user requirements, thereby putting the privacy of the citizen at risk. At the same time, the Internet is changing from a client-server to a collaborative paradigm. Individuals are contributing throughout their life leaving a life-long trace of personal data. This raises substantial new privacy challenges.

Saving digital privacy. By 2008, the European project PRIME (Privacy and Identity Management for Europe) had demonstrated that existing privacy technologies can enable citizens to execute their legal rights to control their personal information in on-line transactions. It had raised considerable awareness amongst stakeholders and has significantly advanced the state of the art in the areas of privacy and identity management. PrimeLife has been building on the momentum created and the results achieved by PRIME to address emerging challenges in the areas of privacy and identity management and really bring privacy and identity management to live:

- A first, short-term goal of PrimeLife was to provide scalable and configurable privacy and identity management in new and emerging internet services and applications such as virtual communities and Web 2.0 collaborative applications.
- A second, longer-term goal of PrimeLife was to protect the privacy of individuals over their whole span of life. Each individual leaves a multitude of traces during a lifetime of digital interactions. Technological advancements facilitate extensive data collection, unlimited storage, as well as reuse and life-long linkage of these digital traces.
- A third goal of PrimeLife was to support privacy and identity management by progressing the state of the art on
  - tools guaranteeing privacy and trust,

  - the usability experience of privacy and identity management solutions,
  - security and privacy policy systems, and
  - privacy-enabling infrastructures.
- The last but certainly important goal of PrimeLife was to disseminate our results and enable their use in real life. We organized interdisciplinary Summer Schools of Privacy, organized and participated in standardization groups and meetings, and made the source code and documentation of most of our prototypes and implementations available for free use.

This Book. After more than three years of work in PrimeLife, this book aims at giving an overview of the results achieved. It is therefore structured into an introduction and six parts covering the most important areas of privacy and identity management considering the life of today: Several aspects of "Privacy in Life" are discussed in Part I, followed by Part II "Mechanisms for Privacy". Part III is dedicated to "Human Computer Interaction (HCI)", and Part IV to "Policy Languages". Part V focuses on "Infrastructures for Privacy and Identity Management," before Part VI "Privacy Live" comes full circle describing how PrimeLife is reaching out to the life of today's and the future's netizens.

Acknowledgements. Editing and writing a multidisciplinary book like this is not possible without many contributors that dedicated their knowledge, expertise, and time to make the work a success. Among the many people that worked on this PrimeLife book, we would like to give a special thanks to:

- The partner organisations and individual researchers in PrimeLife that contributed to this book and the underlying PrimeLife deliverables. They come from seven Member States of the European Union, Switzerland, and the USA.
- Els van Herreweghen who was instrumental in writing and submitting the project proposal and Dieter Sommer who did a wonderful job as coordinator.
- The international team of reviewers that as friends of PrimeLife dedicated their time to improve and streamline the parts of this book. We are particularly grateful to Bart De Decker, Ian Glazer, David-Olivier Jaquet-Chiffelle, Vaclav Matyas, Vincent Naessens, Lasse Øverlier, Jakob Pagter, Michael Pedersen, Claire Vishik, and Jozef Vyskoc for their most valuable comments and suggestions.
- The people who helped to create this book:
  - Michelle Cryer for transforming much of the nerds' English in the draft versions of this book into English.
  - The PrimeLife "Activity Leaders" Katrin Borcea-Pfitzmann, Sandra Steinbrecher, Pierangela Samarati, Gregory Neven, Gökhan Bal, and Marit Hansen for their support and coordination of the respective parts. Gregory also provided the Latex templates and wisdom on how to put the different chapters and parts together into this book.

  - Our colleagues at IBM Research – Zurich, Karlstad University, and Goethe University Frankfurt for keeping our backs covered when we were working on this book.
  - Saskia Werdmüller for the final checking of the manuscript.
  - Christian Rauscher at Springer for helping us with publication of the book.

- The European Commission for funding PrimeLife and our Project Officers Manuel Carvalhosa and Maria-Concepcion Anton-Garcia, their management, Jacques Bus, Jesus Villasante, Thomas Skordas, Gustav Kalbe, and Dirk van Rooy, and the project reviewers Jean-Marc Dinant, Alberto Escudero-Pascual, and Massimo Felici for most valuable feedback and encouragement.
- Last, but certainly not least, all the members of the PrimeLife Reference Group for many inspiring discussions and lots of valuable and helpful feedback.

We hope that this book will contribute to the understanding that digital privacy can be a reality: Many tools exist and are waiting to be deployed in practice.

Zurich, Karlstad, Frankfurt,
March 2011

Jan Camenisch
Simone Fischer-Hübner
Kai Rannenberg

List of Contributors to this Book

Stefano Paraboschi, Gerardo Pelosi, Mario Verdicchio
Università degli Studi di Bergamo, DIIMM
Viale Marconi 25, Dalmine, I-24044

Cornelia Graf, Christina Hochleitner, Manfred Tscheligi, Peter Wolkerstorfer
CURE – Center for Usability Research and Engineering
Modecenterstrasse 17, Vienna, A-1110

Katrin Borcea-Pfitzmann, Jaromir Dobias, Benjamin Kellermann, Stefan Köpsell, Andreas Pfitzmann, Stefanie Pötzsch, Sandra Steinbrecher
Dresden University of Technology, Department of Computer Science
Nöthnitzer Strasse 46, Dresden, D-01187

Marc-Michael Bergfeld, Stephan Spitz
Giesecke & Devrient
Prinzregentenstrasse 159, München, D-81677

Gökhan Bal, Sascha Koschinat, Kai Rannenberg, Christian Weber
Goethe University Frankfurt, T-Mobile Chair of Mobile Business & Multilateral Security Grüneburgplatz 1, Frankfurt/Main, D-60629

Jan Camenisch, Maria Dubovitskaya, Gregory Neven, Franz-Stefan Preiss
IBM Research – Zurich
Säumerstrasse 4, Rüschlikon, CH-8803

Julio Angulo
Karlstad University, Department of Information Systems
Universitetsgatan 2, Karlstad, S-65188

Simone Fischer-Hübner, Hans Hedbom, Tobias Pulls
Karlstad University, Department of Computer Science
Universitetsgatan 2, Karlstad, S-65188

Erik Wästlund
Karlstad University, Department of Psychology
Universitetsgatan 2, Karlstad, S-65188

Filipe Beato, Markulf Kohlweiss, Jorn Lapon, Stefan Schiffner, Karel Wouters
Katholieke Universiteit Leuven, ESAT - COSIC
Kasteelpark Arenberg 10, Leuven, B-3001

Laurent Bussard, Ulrich Pinsdorf
Microsoft EMIC
Ritterstrasse 23, Aachen, D-52072

Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Eros Pedrini, Pierangela Samarati
Università degli Studi di Milano, Dip. di Tecnologie dell'Informazione
Via Bramante 65, Crema, I-26013

Michele Bezzi, Akram Njeh, Stuart Short, Slim Trabelsi
SAP Labs France
805, Avenue du Docteur Maurice Donat, BP 1216, Mougins Cedex, F-06254

Bibi van den Berg, Laura Klaming, Ronald Leenes, Arnold Roosendaal
Universiteit van Tilburg, TILT
Postbus 90153, Tilburg, NL-5000 LE

Marit Hansen, Leif-Erik Holtz, Ulrich König, Sebastian Meissner, Jan Schallaböck, Katalin Storf, Harald Zwingelberg
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstrasse 98, Kiel, D-24103

Carine Bournez, Dave Raggett, Rigo Wenning
World Wide Web Consortium (W3C)
Route des Lucioles, BP 93, Sophia-Antipolis, F-06902

Contents

Part VI Privacy Live