Data-Centric Systems and Applications

Milan Petković · Willem Jonker (Eds.)

Security, Privacy, and Trust in Modern Data Management

With 89 Figures and 13 Tables

Springer

Editors

Milan Petković

Philips Research Europe
High Tech Campus 34
5656 AE Eindhoven
The Netherlands
milan.petkovic@philips.com

Willem Jonker

Philips Research / Twente University
Philips Research Europe
High Tech Campus 34
5656 AE Eindhoven
The Netherlands
willem.jonker@philips.com

Library of Congress Control Number: 2007925047

ACM Computing Classification (1998): D.4.6, E.3, H.2.7, K.6.5

ISBN 978-3-540-69860-9 Springer Berlin Heidelberg New York

Cover Design: KünkelLopka, Heidelberg
Typesetting: by the Editors
Production: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig

Printed on acid-free paper 45/3100/YL 5 4 3 2 1 0

Foreword

Advances in information and communication technologies continue to provide new means of conducting remote transactions. Services facilitated by these technologies are spreading increasingly into our commercial and private spheres. For many people, these services have changed the way they work, communicate, shop, arrange travel, etc. Remote transactions, however, may also open possibilities for fraud and other types of misuse. Hence, the requirement to authorize transactions may arise. Authorization may in turn call for some kind of user authentication. When users have to provide personal information to access services, they literally leave a part of their life on record. As the number of sites where such records are left increases, so does the danger of misuse. So-called identity theft has become a pervasive problem, and a general feeling of unease and lack of trust may dissuade people from using the services on offer.

This, in a nutshell, is one of the major challenges in security engineering today. How to provide services to individuals securely without making undue incursions into their privacy at the same time. Decisions on the limits of privacy intrusions – or privacy protection, for that matter – are ultimately political decisions. Research can define the design space in which service providers and regulators may try to find acceptable tradeoffs between security and privacy.

This book introduces the reader to the current state of privacy-enhancing technologies. In the main, it is a book about access control. An introduction to privacy legislation sets the scene for the technical contributions, which show how access control has evolved to address a variety of requirements that can be found in today's information technology (IT) landscape. The book concludes with an outlook on some of the security and privacy issues that arise in the context of ambient intelligence.

Given current developments in IT that aim to let users access the services they desire wherever they happen to be, or provide the means of monitoring people wherever they happen to be, such a book is timely indeed. It brings together in one place descriptions of specialized techniques that are beyond the scope of textbooks on security. For the security practitioner the book

can serve as a general reference for advanced topics in access control and privacy-enhancing technologies. Last but not least, academics can use it as the basis for specialized courses on those very topics; the research results covered in this book will have a real impact only if they are appreciated by a wider audience. This book plays a valuable part in disseminating knowledge of these techniques.

Hamburg, *Dieter Gollmann*
October 2006

Preface

Information and communication technologies are advancing fast. Processing speed is still increasing at a high rate, followed by advances in digital storage technology, which double storage capacity every year. In contrast, the size of computers and storage has been decreasing rapidly. Furthermore, communication technologies do not lag behind. The Internet has been widely used, as well as wireless technologies. With a few mouse clicks, people can communicate with each other around the world. All these advances have great potential to change the way people live, introducing new concepts like ubiquitous computing and ambient intelligence.

The vision of ubiquitous computing and ambient intelligence describes a world of technology which is present everywhere in the form of smart and sensible computing devices that are able to communicate with one another. The technology is nonintrusive, transparent and hidden in the background. In the ambient intelligence vision, the devices collect, process and share all kinds of information, including user behavior, in order to act in an intelligent and adaptive way.

Although cryptography and security techniques have been around for quite some time, emerging technologies such the ones described above place new requirements on security with respect to data management. As data is accessible anytime anywhere, according to these new concepts, it becomes much easier to get unauthorized data access. Furthermore, it becomes simpler to collect, store, and search personal information and endanger people's privacy.

In the context of these trends this book provides a comprehensive guide to data management technologies with respect to security, privacy, and trust. It addresses the fundamental concepts and techniques in this field, but also devotes attention to advanced technologies, providing a well-balanced overview between basic and cutting-edge technologies. The book brings together issues on security, privacy, and trust, discusses their influences and dependencies. It starts by taking a step back to regain some perspective on the privacy and security issues of the modern digital world. To achieve this, the book not only lists and discusses privacy and security issues, but gives the ethical and legis-

lation background in the context of data storage and processing technologies, as well as technologies that support and implement fair information practices in order to prevent security and privacy violations.

The main goal of the book is, however, to clarify the state of the art and the potential of security, privacy and trust technologies. Therefore, the main part of the book is devoted to secure data management, trust management and privacy-enhancing technologies. In addition, the book aims at providing a comprehensive overview of digital asset protection techniques. The requirements for secure distribution of digital assets are discussed form both the content owner and consumer perspective. After that, the book gives an overview of technologies and standards that provide secure distribution and usage of information, namely digital rights management, copy protection, and watermarking.

Finally, as a viable route towards ambient intelligence and ubiquitous computing can only be achieved if security and confidentiality issues are properly dealt with, the book reviews these newly introduced issues as well as technological solutions to them.

Intended Audience

This book is directed towards several reader categories. First of all, it is intended for those interested in an in-depth overview of information security, privacy and trust technologies. We expect that practitioners will find this book a valuable reference when dealing with these technologies. System architects will find in it an overview of security and privacy issues, which will help them to build systems taking into account security and privacy requirements from the very beginning. System and software developers/engineers will find the theoretical grounds for the design and implementation of security protocols and privacy-enhancing technologies. In addition, the book includes more advanced security and privacy topics including the ones that arise with the concepts of ambient intelligence. As the book covers a balanced mixture of fundamental and advanced topics in security and privacy, it will be of interest to researchers, either those beginning research in this field or those already involved. Last but not least, we have made a considerable effort to make this book appropriate as a course book, primarily for undergraduate, but also for postgraduate students.

Acknowledgements

We would like to acknowledge all the people who have helped us in the completion of this book. It is a result of a concentrated and coordinated effort of 45 eminent authors who presented their knowledge and the ideas in the area of information security, privacy, and trust. Therefore, first of all, we would like

to thank them for their work. Without them, this comprehensive overview of security, privacy and trust technologies in modern data management would have never seen the light of day. Next, we would like to mention Stefano Ceri and Mike Carey. Their comments were helpful in making this a better book. Ralf Gerstner from Springer was very supportive during the editing process. Finaly, special thanks also go to all the reviewers of the book, namely, Klaus Kursawe, Jorge Guajardo, Jordan Chong, and Anna Zych.

Eindhoven, *Milan Petković*
October 2006 *Willem Jonker*

Contents

Part I Introduction

1 Privacy and Security Issues in a Digital World
Milan Petković, Willem Jonker 3

2 Privacy in the Law
Jeroen Terstegge 11

3 Ethical Aspects of Information Security and Privacy
Philip Brey 21

Part II Data and System Security

4 Authorization and Access Control
Sabrina De Capitani di Vimercati, Sara Foresti, Pierangela Samarati . . . 39

5 Role-Based Access Control
Sylvia L. Osborn 55

6 XML Security
Claudio A. Ardagna, Ernesto Damiani, Sabrina De Capitani di Vimercati, Pierangela Samarati 71

7 Database Security
Elisa Bertino, Ji-Won Byun, Ashish Kamra 87

8 Trust Management
Claudio A. Ardagna, Ernesto Damiani, Sabrina De Capitani di Vimercati, Sara Foresti, Pierangela Samarati 103

9 Trusted Platforms
Klaus Kursawe 119

10 Strong Authentication with Physical Unclonable Functions
Pim Tuyls, Boris Škorić 133

Part III Privacy Enhancing

11 Privacy-Preserving Data Mining
Ljiljana Branković, Zahidul Islam, Helen Giggins 151

12 Statistical Database Security
Ljiljana Branković, Helen Giggins 167

13 Different Search Strategies on Encrypted Data Compared
Richard Brinkman 183

14 Client-Server Trade-Offs in Secure Computation
Berry Schoenmakers, Pim Tuyls 197

15 Federated Identity Management
Jan Camenisch, Birgit Pfitzmann 213

16 Accountable Anonymous Communication
Claudia Diaz, Bart Preneel 239

Part IV Digital Asset Protection

17 An Introduction to Digital Rights Management Systems
Willem Jonker 257

18 Copy Protection Systems
Joop Talstra 267

19 Forensic Watermarking in Digital Rights Management
Michiel vd Veen, Aweke Lemma, Mehmet Celik, Stefan Katzenbeisser . . . 287

20 Person-Based and Domain-Based Digital Rights Management
Paul Koster 303

21 Digital Rights Management Interoperability
Frank Kamperman 317

22 DRM for Protecting Personal Content
Hong Li, Milan Petković 333

23 Enhancing Privacy for Digital Rights Management
Milan Petković, Claudine Conrado, Geert-Jan Schrijen, Willem Jonker . 347

Part V Selected Topics on Privacy and Security in Ambient Intelligence

24 The Persuasiveness of Ambient Intelligence
Emile Aarts, Panos Markopoulos, Boris de Ruyter 367

25 Privacy Policies
Marnix Dekker, Sandro Etalle, Jerry den Hartog 383

26 Security and Privacy on the Semantic Web
Daniel Olmedilla 399

27 Private Person Authentication in an Ambient World
Pim Tuyls and Tom Kevenaar 417

28 RFID and Privacy
Marc Langheinrich 433

29 Malicious Software in Ubiquitous Computing
Morton Swimmer 451

Index 467

List of Contributors

Emile Aarts
Philips Research
High Tech Campus 34
Eindhoven, 5656AE
The Netherlands
emile.aarts@philips.com

Claudio A. Ardagna
Università degli Studi di Milano
Via Bramante 65
26013 Crema (CR) – Italia
ardagna@dti.unimi.it

Elisa Bertino
Purdue University
305 N. University Street
West Lafayette
IN 47907-2107, USA
bertino@cs.purdue.edu

Ljiljana Branković
The University of Newcastle
Callaghan, NSW 2308, Australia
ljiljana.brankovic@newcastle.edu.au

Philip Brey
University of Twente
Postbox 217
7500AE Enschede
The Netherlands
p.a.e.brey@utwente.nl

Richard Brinkman
University of Twente
Postbus 217
7500AE Enschede
The Netherlands
brinkman@cs.utwente.nl

Ji-Won Byun
Purdue University
305 N. University Street
West Lafayette
IN 47907-2107, USA
byunj@cs.purdue.edu

Jan Camenisch
IBM Zurich Research Lab
Säumerstrasse 4,
CH-8803 Rüschlikon, Switzerland
jca@zurich.ibm.com

Sabrina De Capitani di Vimercati
Università degli Studi di Milano
Via Bramante 65
26013 Crema (CR) – Italia
decapita@dti.unimi.it

Mehmet Celik
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
mehmet.celik@philips.com

Claudine Conrado
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
claudine.conrado@philips.com

Ernesto Damiani
Università degli Studi di Milano
Via Bramante 65
26013 Crema (CR) – Italia
damiani@dti.unimi.it

Marnix Dekker
TNO ICT
Postbus 5050
2600GB Delft, The Netherlands
marnix.dekker@tno.nl

Claudia Diaz
K.U.Leuven ESAT-COSIC
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee, Belgium
claudia.diaz@esat.kuleuven.be

Sandro Etalle
University of Twente
Postbus 217
7500AE Enschede
The Netherlands
sandro.etalle@utwente.nl

Sara Foresti
Università degli Studi di Milano
Via Bramante 65
26013 Crema (CR) – Italia
foresti@dti.unimi.it

Helen Giggins
The University of Newcastle
Callaghan, NSW 2308, Australia
helen.giggins@newcastle.edu.au

Jerry den Hartog
University of Twente
Postbus 217
7500AE Enschede
The Netherlands
jerry.denhartog@utwente.nl

Md. Zahidul Islam
The University of Newcastle
Callaghan
NSW 2308
Australia
zahid.islam@newcastle.edu.au

Willem Jonker
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
willem.jonker@philips.com

Frank Kamperman
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
frank.kamperman@philips.com

Ashish Kamra
Purdue University
305 N. University Street
West Lafayette
IN 47907-2107
USA
akamra@cs.purdue.edu

Stefan Katzenbeisser
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
stefan.katzenbeisser@philips.com

Tom Kevenaar
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
tom.kevenaar@philips.com

Paul Koster
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
r.p.koster@philips.com

Klaus Kursawe
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
klaus.kursawe@philips.com

Marc Langheinrich
Institute for Pervasive Computing
ETH Zurich
8092 Zurich, Switzerland
langhein@inf.ethz.ch

Aweke Lemma
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
aweke.lemma@philips.com

Hong Li
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
hong.r.li@philips.com

Panos Markopoulos
TU Eindhoven
P.O. Box 513
5600 MB Eindhoven
The Netherlands
p.markopoulos@tue.nl

Daniel Olmedilla
L3S Research Center and
University of Hannover
Expo Plaza 1, 30539
Hannover, Germany
olmedilla@L3S.de

Sylvia L. Osborn
The University of Western Ontario
London, ON, N6A 5B7
Canada
sylvia@csd.uwo.ca

Milan Petković
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
milan.petkovic@philips.com

Birgit Pfitzmann
IBM Zurich Research Lab
Säumerstrasse 4
CH-8803 Rüschlikon, Switzerland
bpf@zurich.ibm.com

Bart Preneel
K.U.Leuven ESAT-COSIC
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.be

Boris de Ruyter
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
boris.de.ruyter@philips.com

Pierangela Samarati
Università degli Studi di Milano
Via Bramante 65
26013 Crema (CR) – Italia
samarati@dti.unimi.it

Berry Schoenmakers
TU Eindhoven
P.O. Box 513
5600MB Eindhoven
The Netherlands
berry@win.tue.nl

Geert-Jan Schrijen
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
geert.jan.schrijen@philips.com

Morton Swimmer
IBM Zurich Research Lab
Säumerstrasse 4
CH-8803 Rüschlikon, Switzerland
bpf@zurich.ibm.com

Boris Škorić
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
boris.skoric@philips.com

Joop Talstra
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
joop.talstra@philips.com

Jeroen Terstegge
Royal Philips
Groenewoudseweg 1
PO Box 218
5600MD Eindhoven
The Netherlands
jeroen.terstegge@philips.com

Pim Tuyls
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
pim.tuyls@philips.com

Michiel van der Veen
Philips Research Europe
HighTech Campus 34
5656AE Eindhoven
The Netherlands
michiel.van.der.veen@philips.com