

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Simone Fischer-Hübner

IT-Security and Privacy

Design and Use of
Privacy-Enhancing Security Mechanisms



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Author

Simone Fischer-Hübner
Karlstad University
Department of Computer Science
Universitetsgatan 1, 651 88 Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fischer-Hübner, Simone:
IT-security and privacy : design and use of privacy enhancing security
mechanisms / Simone Fischer-Hübner. - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo :
Springer, 2001
(Lecture notes in computer science ; Vol. 1958)
ISBN 3-540-42142-4

CR Subject Classification (1998): C.2, D.4.6, K.6.5, E.3, H.2.0, K.4

ISSN 0302-9743

ISBN 3-540-42142-4 Springer-Verlag Berlin Heidelberg New York

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author
Printed on acid-free paper SPIN 10781014 06/3142 5 4 3 2 1 0

Foreword

In public debates about **potential impacts** of contemporary Information and Communication Technologies (ICTs), **invasion of “privacy” and misuse of personal data** are often regarded as being amongst the most evident negative effects of ICTs which should be carefully analysed and controlled. Computing experts and informaticians often use the term **“data protection”** as synonymous with “privacy” although this usage is somewhat misleading: the main task is NOT to protect the data but it is the **task to protect the personal sphere** represented by the data and their relations associated with a person (sometimes called the “data shadow” of a person’s privacy).

Indeed, the term “data protection” tends to hide basic problems which have to be solved to technically protect the “data shadow” of a person’s “private sphere”. While “data protection” assumes that data have been taken and stored, an analysis of person’s privacy concerns may require that related data should on no account be taken and stored. Therefore, the term “data protection” is too technically reductive to be used synonymously for privacy.

The consistent inadequate usage of the term “data protection” is another illustration of the validity of Joseph Weizenbaum’s metaphor (in his book “Computer Power and Human Reasoning”) according to which computer scientists tend to search for some solutions in the light of a lantern, whereas the key lies in the shadow. Indeed, it is comparably easy to describe how to technically protect data, whether related to a person, an enterprise or any other entity. Several models exist for restricting access to any data, either on a “discretionary” or “mandatory” basis (DAC, MAC), either built into the kernel of an operating system (“Reference Monitor”) or into some outer shell. Some models may also distinguish between the roles a user of stored data actually plays (RBAC), and a refined model may also include tasks which a user actually has to perform upon such data (a valuable contribution of the author of this book). “Auditing” provides adequate means to control whether personal data are used according to prescriptions, such as rights of users or capabilities of related IT processes. All these models are quite easily implemented (although it is also easy to switch such technical protection off).

Beyond such technical methods, models, and tools, it is significantly more difficult to describe **basic requirements and means to protect the “data shadow” of a person**. Some such requirements can be found in the privacy laws which have been passed in several countries, though on different levels. Some degree of harmonization is available in the European Union, based on its Data Protection Directive, but there still exist many problems in the exchange of personal data with areas with different (or no) legal requirements.

Requirements for privacy protection may depend upon the legal basis of privacy in a particular country. In Germany where privacy is regarded as some quasi-constitutional **“right for informational self-determination”**, such requirements are concerned with the **necessity** of data collection and processing, **purpose specification**

and **purpose binding**, and **the transparency** of personal data protection. In addition, directives of the European Union and OECD also require **lawfulness and fairness**. Based on the different legal systems, there are sufficient stipulations on the legal side regarding which requirements must be legally fulfilled to store, process, and communicate personal data.

For a long time, these legal requirements were almost disregarded by the ICT community. Until very recently, there was no basic model for privacy-related requirements which implementations and usage of related information systems must fulfill. It is the specific **value of Simone Fischer-Hübner's work** (published in this book covering her habilitation thesis), that a first model is now available which permits the description of requirements derived from legal concepts.

Moreover, the author does not simply present her suggestions as a collection of principles and technical requirements. Besides developing a "privacy-friendly concept of data protection", she also presents it as a formal model, the implementation of which (when done properly) may help to prove that privacy requirements have indeed been implemented in some software. The demonstration of the model presented in this book is also embedded in contemporary concepts of IT Security, as seen by the description of its realization within LaPadula's Generalized Framework for Access Control. Consequently, implementations of her model will - if done correctly - make the related software not only adaptable to contemporary ITSEC concepts but at the same time "**conforming with law**" and "**privacy-friendly**". She also convincingly counters any argument that such models are "just theoretical and hardly to be implemented": she demonstrates that and how her model can be implemented on a relevant platform.

This book can – and hopefully will – become the foundation of a new way to model and consequently implement user requirements into ICT systems which conform better than before with human principles (starting but not ending with privacy). In this sense, it is my sincere hope that this book becomes really successful.

November 2000

Dr. Klaus Brunnstein
Professor for Application of Informatics
University of Hamburg

Preface

In the Global Information Society, the individual's privacy is seriously endangered and is becoming more and more an international problem. An international harmonisation of privacy legislation is needed but is hardly achievable due to cultural differences. Therefore, privacy commissioners are demanding that privacy should be a design criterion and that more privacy-enhancing technologies have to be designed, implemented and used. In addition to privacy technologies for the protection of users, there is also a need for privacy enhancing technologies for protecting the data subjects, who are not necessarily system users.

In this thesis, the related areas of privacy, IT-security and privacy-enhancing technologies are presented, elaborated, analysed and discussed. The central part of this thesis is the presentation of a formal task-based privacy model, which can be used to technically enforce legal privacy requirements such as the necessity of personal data processing and purpose binding. In addition, it is specified how the privacy model policy has been implemented together with other security policies according to the Generalized Framework for Access Control (GFAC).

This thesis was submitted as a habilitation thesis at Hamburg University in Germany, where it was accepted by the habilitation committee in December 1999. Subsequently, updates have been made to reflect recent developments.

A number of persons have supported me during the time in which I wrote and completed this thesis. I would like to give my thanks to all of them:

I am especially grateful to Prof. Dr. Klaus Brunnstein, who introduced me to the field of IT security and taught me the importance of taking an holistic view. The discussions I had with him, his ideas, motivating spirit and practical support have been very valuable to me.

I also want to express my gratitude to my colleagues at the Copenhagen Business School (CBS). In particular, I thank Prof. Gert Bechlund, who invited me to be a Guest Professor at the Institute of Computer and System Sciences (DASY) at CBS from fall 1994 to spring 1995, and Prof. Lars Frank, for the interesting discussions we had while we were working together at CBS. I also thank CBS for having funded my research during the time of my guest professorship.

I also owe special thanks to my colleague Dr. Louise Yngström, who has always been a valuable discussion partner and good friend to me. I especially want to thank her for initiating my invitation as a Guest Professor at the Department of Computer and System Sciences (DSV) at Stockholm University / KTH, which was financed by the Swedish Research Council. At DSV, I also found time for completing this thesis. Therefore I also want to thank DSV for all of its support and for providing a very pleasant working atmosphere.

I also want to thank my former student and colleague Amon Ott, with whom I worked closely during the phase of specification and implementation of my privacy

policy. He was mainly responsible for RSBAC system implementation and discussed with me my system specification. I have enjoyed working with him very much.

I would also like to thank Dr. Michael Sobirey for stimulating discussions and cooperation. Furthermore, I thank my colleagues Dr. Kathrin Schier, Fredrik Björck and Kjell Näckros for discussions, support and friendship, as well as all my other colleagues from IFIP Working Group 9.6 for having been knowledgeable discussion partners.

I am also grateful to a friend of my family, William Watts, who has polished my English. Any mistakes that I might have introduced by modifying the text after he had done his corrections are entirely my own.

I also want to thank the members of the habilitation committee at Hamburg University, and also in particular the external evaluators Prof. Dr. Dr. Gerald Quirchmayr (Univ. Vienna), Prof. Dr. Waltraut Gerhardt (TU Delft) and Prof. Dr. Andreas Pfitzmann (TU Dresden) as well as Prof. Dr. Klaus Brunnstein, who acted as an internal evaluator, for all the work and time they had to spend reading and evaluating this thesis.

Last but not least, I would like to thank my family to whom I dedicate this work. I am most grateful to my beloved parents Hermann and Helga Fischer-Hübner, who have always supported and motivated me. My father as a dedicated lawyer, who was committed to his profession and clients, raised my interest in law and taught me the importance of justice. Finally, I want to express my special thanks to my dear husband Etamar, who was always there for me with love, patience and care.

September 2000

Simone Fischer-Hübner

Table of Contents

1. Introduction	1
2. Privacy in the Global Information Society	5
2.1 Definition of Privacy and Data Protection	5
2.2 Historical Perspective on Data Protection Legislation	6
2.3 Privacy Principles of the German Census Decision	8
2.4 Basic Privacy Principles.....	10
2.5 The EU Directive on Data Protection.....	11
2.6 German Data Protection Legislation	14
2.6.1 The German Federal Data Protection Act (Bundesdatenschutzgesetz)	14
2.6.2 Data Protection Regulations for Information and Telecommunication Services	17
2.7 Threats to Privacy in the Global Networked Society	18
2.7.1 Privacy Threats at Application Level	18
2.7.2 Privacy Threats at Communication Level	20
2.7.3 Insecure Technologies.....	23
2.8 Problems of an International Harmonisation of Privacy Legislation	24
2.9 The Need for Privacy Enhancing Technologies.....	30
2.10 The Importance of Privacy Education.....	31
2.11 Conclusions.....	32
3. IT-Security	35
3.1 Definition.....	35
3.2 Security Models	38
3.2.1 Harrison-Ruzzo-Ullman Model.....	40
3.2.2 Bell LaPadula Model	41
3.2.3 Unix System V/MLS Security Policy.....	46
3.2.4 Biba Model.....	47
3.2.5 Lattice Model of Information Flow.....	49

- 3.2.6 Noninterference Security Model 51
- 3.2.7 Clark-Wilson Model..... 52
- 3.2.8 Chinese Wall Model..... 56
- 3.2.9 Role-Based Access Control Models..... 58
- 3.2.10 Task-Based Authorisation Models for Workflow 65
 - 3.2.10.1 Workflow Authorisation Model (WAM)..... 66
 - 3.2.10.2 Task-Based Authorisation Controls (TBAC) 68
- 3.2.11 Security Models for Object-Oriented Information Systems 68
 - 3.2.11.1 The Authorisation Model by Fernandez et al. 69
 - 3.2.11.2 The Orion Authorisation Model 69
 - 3.2.11.3 The DORIS Personal Model of Data 70
 - 3.2.11.4 Further Relevant Research..... 71
- 3.2.12 Resource Allocation Model for Denial of Service Protection 72
- 3.2.13 Multiple Security Policies Modelling Approaches..... 75
 - 3.2.13.1 The Generalised Framework for Access Control (GFAC) 75
 - 3.2.13.2 The Multipolicy Paradigm and Multipolicy Systems 78
- 3.3 Basic Security Functions and Security Mechanisms..... 78
 - 3.3.1 Identification and User Authentication 78
 - 3.3.2 Access Control 79
 - 3.3.3 Auditing..... 80
 - 3.3.4 Intrusion Detection Systems..... 81
 - 3.3.5 Object Reuse Protection 83
 - 3.3.6 Trusted Path 83
 - 3.3.7 Cryptography..... 83
 - 3.3.7.1 Foundations 83
 - 3.3.7.2 Symmetric Algorithms 85
 - 3.3.7.3 Asymmetric Algorithms 87
 - 3.3.7.4 Hash Functions 88
 - 3.3.7.5 Certificates..... 88
- 3.4 Security Evaluation Criteria..... 90
 - 3.4.1 The Rainbow Series (Orange Book et al.)..... 91
 - 3.4.2 European Initiatives..... 93
 - 3.4.2.1 Overview 93
 - 3.4.2.2 The German Green Book..... 94
 - 3.4.2.3 The Information Technology Security Evaluation Criteria (ITSEC) 94
 - 3.4.3 North American Initiatives 96
 - 3.4.3.1 CTCPEC..... 96
 - 3.4.3.2 MSFR 96
 - 3.4.3.3 Federal Criteria..... 97
 - 3.4.4 International Harmonisation..... 97
 - 3.4.4.1 ISO Initiatives (ISO/IEC-ECITS)..... 97
 - 3.4.4.2 The Common Criteria..... 97
 - 3.4.5 Shortcomings of IT Security Evaluation Criteria 101
- 3.5 Conflict between IT Security and Privacy 102
 - 3.5.1 Privacy Implications of IT Security Mechanisms 102

3.5.2	A Holistic Approach to a Privacy-Friendly Design and Use of Security Mechanisms	104
-------	---	-----

4. Privacy-Enhancing Technologies107

4.1	Privacy-Enhancing Security Aspects	107
4.1.1	Privacy-Enhancing Security Aspects for Protecting the User Identities	107
4.1.1.1	Anonymity	108
4.1.1.2	Unobservability	109
4.1.1.3	Unlinkability	110
4.1.1.4	Pseudonymity	110
4.1.2	Privacy-Enhancing Security Criteria for Protecting the Usee Identities	112
4.1.2.1	Depersonalisation	112
4.1.2.2	The Risk of Re-identification	113
4.1.3	Privacy-Enhancing Security Aspects for Protecting Personal Data	119
4.2	System Concepts for Protecting User Identities	120
4.2.1	The Identity Protector	120
4.2.2	Protecting User Identities at Communication Level	121
4.2.2.1	Recipient Anonymity through Message Broadcast and Implicit Addresses	122
4.2.2.2	Dummy Traffic	122
4.2.2.3	DC-Nets	123
4.2.2.4	Mix-Nets	127
4.2.2.5	Crowds	134
4.2.3	Protecting User Identities at System Level	135
4.2.3.1	Pseudonymous System Accounts	135
4.2.3.2	Anonymous System Access and Use through Authorisation Certificates	135
4.2.4	Protecting User Identities at Application Level	137
4.2.4.1	Prepaid Cards	137
4.2.4.2	Untraceable Electronic Money through Blind Signatures	137
4.2.5	Protecting User Identities in Audit Data through Pseudonymous Auditing	141
4.2.5.1	Functionality of Pseudonymous Auditing	142
4.2.5.2	Pseudonymisation of User Identifying Data in Audit Records	143
4.2.5.3	Pseudonymisation Techniques	145
4.2.6	Protecting User Identities from other Users and Services	145
4.2.7	The Need for Anonymity and the Problem of Its Potential Misuse	146
4.3	System Concepts for Protecting Usee Identities - Inference Controls for Statistical Database Systems	147

4.4	System Concepts and Mechanisms for Protecting Personal Data	152
4.4.1	Steganographic Systems.....	153
4.4.2	Access Control Models for Personal Data Protection	156
4.4.2.1	Privacy Criteria for Security Models	156
4.4.2.2	Privacy Evaluation of Security Models	157
4.5	Privacy Evaluation of IT Security Evaluation Criteria	163
4.6	Conclusions.....	164
5.	A Task-Based Privacy Model	167
5.1	Introduction.....	167
5.2	Model Description.....	167
5.2.1	Model Elements (State Variables).....	167
5.2.2	Model Invariants and Constraints (Privacy Properties).....	174
5.2.2.1	Privacy Invariants.....	174
5.2.2.2	Privacy Constraints	175
5.2.3	Model Rules (State Transition Functions).....	175
5.2.3.1	General Transition Functions	176
5.2.3.2	Privileged Transition Functions	178
5.3	Information Flow Control	186
5.4	Revocation of Authorisations.....	194
5.5	Example: Application of the Privacy Model in a Hospital Information System.....	198
5.6	Analysis of the Privacy Model.....	199
6.	Specification and Implementation of the Privacy Policy Following the Generalised Framework for Access Control-Approach.....	201
6.1	Introduction	201
6.2	The Specification of the Privacy Policy Rules Component	203
6.2.1	Access Control Information (ACI).....	204
6.2.2	Access Control Enforcement Facility (AEF) and Its Interface to ADF	210
6.2.3	Access Control Decision Facility (ADF)	227
6.3	Implementation	253
6.3.1	RSBAC Implementation	253
6.3.2	Integration of Heuristic Policy Rules.....	254
6.4	Outlook....	256
7.	Concluding Remarks	259

Appendix A: Formal Mathematical Privacy Model	261
1. Model Components.....	261
2. Privacy-Oriented System.....	264
3. Theorems	268
4. Formal Definition of the Model Rules.....	289
5. Proofs	304
 Appendix B: Implementation of a Hospital Scenario as a Demonstration Example	 325
 References.....	 331