

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 Model261

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 Example325**

References.....331

IT-Security and Privacy
Design and Use of Privacy-Enhancing Security
Mechanisms
Fischer-Hübner, S.
2001, XIV, 358 p., Softcover
ISBN: 978-3-540-42142-9