
Contents

1	Introduction - The Scope of the Work and its Methodology	1
1.1	Defining Security and Privacy	2
1.2	The Importance of Standards	4
1.3	Technological Issues	7
1.4	Organization and the Human Factor	8
1.5	Legal Frameworks	9
1.6	Before Proceeding Further	10
2	Organization, Security and Privacy	13
2.1	Recent History of the Field	13
2.2	Frameworks Level	15
2.2.1	Assets	17
2.2.2	Threats	17
2.2.3	Vulnerabilities	18
2.2.4	Risks and Impacts	18
2.2.5	Safeguards and Residual Risk	18
2.2.6	The Concept of Security Management Processes	19
2.3	Techniques for ISs Security Management	19
2.3.1	Security Objectives and Strategies	20
2.3.2	Security Related Organizational Issues	21
2.3.3	Risk Analysis	21
2.3.4	Safeguards Selection, Security Policy Definition and its Realization	26
2.3.5	Supervision and Incident Handling	27
2.4	Particular Implementations Level	27
2.4.1	General Hints for Selection of Safeguards	28
2.4.2	Organizational Safeguards	29
2.4.3	Personnel Security	29
2.4.4	Physical and Environmental Security	30
2.4.5	Access Control, Communications and Operations Security	31

2.4.6	ISs Development, Maintenance, and Monitoring	33
2.4.7	Incident Handling	36
2.4.8	Business Continuity Planning	36
2.4.9	Compliance and Auditing	37
2.4.10	Security Awareness	38
2.5	Standardized Safeguard Templates	39
2.5.1	Organizational Safeguard Templates	39
2.5.2	Technology Compliance Safeguards	39
3	Security Technology: Concepts and Models	43
3.1	Security Mechanisms	44
3.1.1	Pseudorandom Number Generators	44
3.1.2	One-way Hash Functions	45
3.1.3	Symmetric Algorithms	47
3.1.4	Asymmetric Algorithms	51
3.1.5	Steganography and Watermarking	54
3.2	Cryptographic Protocols	56
3.2.1	A Brief Overview of Computer Communications	57
3.2.2	Security Services	59
3.2.3	Models of Security Services	59
3.2.4	The Relationships Between Security Services	64
3.3	Key Management	66
3.3.1	Key Generation	66
3.3.2	Key Distribution	66
3.3.3	Complementary Key Management Activities	68
3.4	Security Infrastructure	69
3.4.1	Public Key Infrastructure	69
3.4.2	Authentication and Authorization Infrastructure	75
3.4.3	Network Layer Security - IPSec	78
3.4.4	Secure Sockets Layer and Transport Layer Security	91
3.4.5	Secure/Multipurpose Internet Mail Extensions	95
3.4.6	One-time Password Systems	100
3.4.7	Firewalls	101
3.4.8	Intrusion Detection Systems	105
3.4.9	Extensible Markup Language Security	107
3.4.10	Smart cards	115
3.4.11	Biometrics Based Technology	117
3.5	Security Services as the Basis for e-Business Processes	120
3.5.1	Electronic Payment Systems	120
3.5.2	Web Services	122
3.6	Privacy Enabling Technologies	131
3.7	A Different Paradigm - Wireless Networking	133

4	Legal Aspects of ISs Security and Privacy	137
4.1	Cryptography in General	137
4.2	Digital Signatures	140
4.3	Privacy Issues	141
4.3.1	Privacy and Electronic Communications	143
4.3.2	Workplace Privacy	144
4.3.3	Spamming	145
4.3.4	Electronic Tracking Technologies	146
4.3.5	Identity Theft	146
4.4	ISs and Software Liability	146
4.5	Intellectual Property Rights	148
4.6	Computer Forensics	149
5	Where Are We Headed?	151
6	Appendix	155
6.1	Brief Mathematical Preliminaries	156
6.1.1	Information Theory	156
6.1.2	Complexity Theory	161
6.1.3	Abstract Algebra	162
6.1.4	Number Theory	163
6.1.5	Computing Inverses and Exponentiation in \mathbb{Z}_n	167
6.1.6	Computational Complexities in \mathbb{Z}_n	168
6.2	Cryptographic Primitives	169
6.2.1	One-way Hash Functions	169
6.2.2	Pseudorandom Number Generators	174
6.2.3	Triple DES	175
6.2.4	RSA Algorithm	183
6.2.5	Diffie-Hellman Key Agreement	184
6.3	Formal Methods	185
6.3.1	Overview of Formal Methods	185
6.3.2	Introduction to Logic BAN	186
6.3.3	Language Z Overview	193
6.3.4	Emerging Formal Methods	198
6.4	Socio-Technical Systems Modeling and Simulation	198
6.4.1	Business Dynamics	199
6.4.2	Agent Technologies	205
	Further Reading	209
	Listing of the Simulation Model	211
	References	213



<http://www.springer.com/978-3-540-28103-0>

Managing Information Systems Security and Privacy

Trcek, D.

2006, XIII, 234 p., Hardcover

ISBN: 978-3-540-28103-0