
Contents

1	Introduction	1
1.1	Motivation	1
1.2	Chapter Structure	2
	References	4
2	Basics of Information Security	5
2.1	Motivation	7
2.1.1	Information Security	8
2.1.2	Study Findings	10
2.2	Security and Security Objectives	14
2.2.1	Information Security—Characteristics—Protection Goals	16
2.2.2	Foundations of Information Security	19
2.2.3	Definitions Related to Information Security	22
2.2.4	Social Engineering	23
2.2.4.1	Social Engineering—Examples	24
2.2.4.2	Social Engineering—Targets of Attack	27
2.2.5	Bug Bounty Programs—Honeypot	28
2.2.5.1	Bug Bounty Program	28
2.2.5.2	Honeypot	29
2.3	Processing Security	29
2.3.1	Technical security measures	30
2.3.2	Organizational Security Measures	30
2.3.3	Organization and Compliance	31
2.3.4	Gathering Information	31
2.3.5	Self-Assessment	31
2.3.6	Test Strategies	32
2.3.7	Turning Point after Stuxnet	34
2.4	NIS Directive	34
2.5	Summary	37
	References	38

3	Data Protection (Privacy)	41
3.1	Motivation/Origin	42
3.1.1	Basic Principles of Protection: Concepts	42
3.1.2	Data Protection: History	43
3.1.3	Privacy: Characteristics and Privacy Objectives	45
3.2	Basis of the EU-GDPR: Federal Data Protection Act n. F.	46
3.2.1	Federal Data Protection Act n. F.	46
3.2.2	EU General Data Protection Regulation	47
3.2.3	ePrivacy: Telecommunications-Telemedia-Data Protection Act.	48
3.2.4	Personal Data	50
3.2.5	Legality of Processing	51
3.3	Important Articles of the EU-GDPR	52
3.3.1	Principles for the processing of personal data	53
3.3.2	Conditions for Consent	54
3.3.3	Security of Processing	54
3.3.4	Rights of the Data Subject	55
3.3.5	Data Protection Impact Assessment.	56
3.3.6	General Conditions for the Imposition of Fines.	57
3.4	Privacy Engineering—Privacy-by-Design	58
3.4.1	Privacy Engineering	58
3.4.2	Seven fundamental principles: Privacy-by-Design (PbD)	60
3.4.3	Privacy Strategies	64
3.5	Privacy-Enhancing-Technologies (PET)	67
3.6	Privacy Risk Model	69
3.6.1	Privacy Risk Analysis.	70
3.6.2	Privacy Threat Modeling: LINDDUN	72
3.7	Data Protection Framework	74
3.8	Summary	75
	References.	78
4	Functional Safety (Safety)	81
4.1	Motivation	81
4.2	Goals—Functional Safety—Characteristics	83
4.3	Interface Functional Safety—Cybersecurity	88
4.3.1	Interfaces in the Automotive Safety Standard	89
4.3.2	Related Analysis Methods	91
4.3.3	SOTIF—Safety of the intended functionality	92
4.3.4	STPA—Systems Theoretic Process Analysis.	93
4.3.5	Artificial Intelligence	94

4.4	Summary	94
	References.....	96
5	Information/Cybersecurity Standards	97
5.1	Security Development Lifecycle: Standards	98
5.1.1	Microsoft Security-Development-Lifecycle (SDL).....	99
5.1.2	IEEE Cyber Security—Design Flaws	100
5.1.2.1	The Top 10 Design Flaws	101
5.1.2.2	Countermeasures to Avoid the Top 10 Design Flaws.....	101
5.1.3	Automotive SPICE®.....	103
5.2	Security Standards	105
5.2.1	SAE International J3061™ ISO/SAE 21434.....	105
5.2.2	FIPS PUB 199/FIPS PUB 200/NIST SP 800-53.....	107
5.2.2.1	FIPS PUB 199—Security Categorization.....	107
5.2.2.2	FIPS PUB 200—Minimum Security Requirements	108
5.2.3	NIST SP 800-Series.....	109
5.2.4	ISA/IEC 62443—IT Security for Networks and Systems.....	110
5.2.4.1	ISA/IEC 62443—Objectives.....	110
5.2.4.2	ISA/IEC 62443—Structure of the Standard Series. . .	112
5.2.4.3	ISA/IEC 62443—Foundational Concepts (Foundational Requirements)	113
5.2.5	27k-Family—Information Security	118
5.2.5.1	ISO/IEC 27001—Information Security Management	119
5.2.5.2	ISO/IEC 27005 Security Risk Management.....	119
5.2.5.3	ISO/IEC 27701—Data Protection Management System.....	119
5.2.6	TISAX—Automotive ISMS.....	120
5.2.7	UNECE/NHTSA—Automotive Regulations.....	121
5.2.8	IEC 15480—Common Criteria	123
5.2.9	RTCA DO 326-A—Aviation Security	126
5.2.10	EU Cybersecurity Act	127
5.3	Summary	128
5.3.1	Secure Software Engineering.....	128
5.3.2	Challenges and Measures.....	129
	References.....	130
6	Hacking	133
6.1	Mindset	134
6.2	Hacking Examples.....	137

6.2.1	Google Hacking	137
6.2.2	Password Hacking	138
6.3	Automotive Hacking Example.	139
6.3.1	Connectivity makes it Possible	140
6.3.2	Example: Roll-Jam Technique (Replay Attack).	142
6.3.3	Example: (Key-) Relay-Station Attack	143
6.4	Cyber Kill Chain	144
6.5	Summary	146
	References.	146
7	Risk Assessment	149
7.1	Overview	150
7.1.1	Principles	151
7.1.2	Framework	151
7.1.3	Process	152
7.1.4	Risk Criteria.	154
7.2	Automotive TARA according to ISO/SAE 21434.	155
7.2.1	Identification of Values to be Protected	155
7.2.2	Identification of Threat Scenarios	156
7.2.3	Determining the Severity of Impact.	158
7.2.4	Analysis of Attack Paths	158
7.2.5	Determining the Feasibility of Attacks	159
7.2.6	Risk Assessment.	160
7.2.7	Risk Treatment Decision	161
7.3	Security Risk Assessment according to ISA/IEC 62443	161
7.4	Risk assessment according to ISO/IEC 27005.	163
7.5	Risk assessment according to NIST SP 800-30.	164
7.6	Risk Assessment according to HEAVENS.	166
7.6.1	Threat Analysis	168
7.6.2	Risk Assessment.	168
7.6.3	Security Requirements.	169
7.7	Threat Modeling: STRIDE	170
7.7.1	STRIDE-per-Element.	170
7.7.2	STRIDE-per-Interaction.	171
7.8	Summary	172
	References.	173
8	IT Service Management	175
8.1	Motivation (Embedding)	178
8.2	ITIL and COBIT	179
8.2.1	ITIL—IT Infrastructure Library.	179
8.2.2	COBIT—Control Objectives for Information and Related Technology.	180

Contents

xi

8.3

27k—Information Security Management System

181

8.4

IT Baseline Protection Compendium.

181

8.4.1

BSI Standards for Implementation.

183

8.4.2

BSI Risk Analysis

186

8.5

The IT Security Officer

187

References.

189

9

Appendix: Control Families.

191

9.1

Control families for Security and Privacy

192

References.

197

Glossary

199