

Table of Contents

Preface	xxii
Part I Overview	1
Chapter 1: Security and Cryptography Concepts	2
1.1 Cybersecurity, Information Security, and Network Security	2
Security Objectives	3
The Challenges of Information Security	5
1.2 Security Attacks	6
Passive Attacks	8
Active Attacks	8
1.3 Security Services	10
Authentication	10
Access Control	11
Data Confidentiality	11
Data Integrity	11
Nonrepudiation	12
Availability Service	12
1.4 Security Mechanisms	12
1.5 Cryptographic Algorithms	13
Keyless Algorithms	14
Single-Key Algorithms	14
Two-Key Algorithms	15
1.6 Symmetric Encryption	15
1.7 Asymmetric Encryption	17
1.8 Cryptographic Hash Functions	20
1.9 Digital Signatures	22
1.10 Practical Considerations	23
Selection of Cryptographic Algorithms and Key Lengths	23
Implementation Considerations	24

Lightweight Cryptographic Algorithms	24
Post-Quantum Cryptographic Algorithms	25
1.11 Public-Key Infrastructure.....	25
Public-Key Certificates	25
PKI Architecture	27
1.12 Network Security.....	29
Communications Security.....	29
Device Security	30
1.13 Key Terms and Review Questions.....	30
Key Terms	30
Review Questions	31
1.14 References	31
Chapter 2: Information Privacy Concepts	32
2.1 Key Privacy Terminology	32
2.2 Privacy by Design.....	35
Privacy by Design Principles.....	35
Requirements and Policy Development.....	37
Privacy Risk Assessment.....	37
Privacy and Security Control Selection	39
Privacy Program and Integration Plan	40
2.3 Privacy Engineering.....	41
Privacy Implementation	44
System Integration.....	44
Privacy Testing and Evaluation	45
Privacy Auditing and Incident Response	45
2.4 Privacy and Security.....	46
Areas of Overlap Between Security and Privacy	46
Trade-Offs Between Security and Privacy	48
2.5 Privacy Versus Utility	48

2.6	Usable Privacy.....	49
	Users of Privacy Services and Functions	50
	Usability and Utility	50
2.7	Key Terms and Review Questions.....	50
	Key Terms	50
	Review Questions	51
2.8	References	51
Part II Privacy Requirements and Threats		53
Chapter 3: Information Privacy Requirements and Guidelines		54
3.1	Personally Identifiable Information and Personal Data	55
	Sources of PII.....	57
	Sensitivity of PII	58
3.2	Personal Information That Is Not PII	59
3.3	Fair Information Practice Principles	63
3.4	Privacy Regulations.....	66
	European Union	66
	U.S. Privacy Laws and Regulations.....	67
3.5	Privacy Standards	68
	International Organization for Standardization (ISO).....	69
	National Institute of Standards and Technology	77
3.6	Privacy Best Practices	88
	Information Security Forum (ISF)	88
	Cloud Security Alliance (CSA).....	90
3.7	Key Terms and Review Questions.....	91
	Key Terms	91
	Review Questions	91
3.8	References	92

Chapter 4: Information Privacy Threats and Vulnerabilities	94
4.1 The Evolving Threat Environment.....	95
Overall Impact of Advances in Technology.....	95
Repurposing Collected Data.....	96
Means of Collection of PII.....	96
4.2 Privacy Threat Taxonomy	97
Information Collection.....	98
Information Processing	98
Information Dissemination	98
Invasions	99
4.3 NIST Threat Model	100
4.4 Threat Sources	105
4.5 Identifying Threats.....	106
4.6 Privacy Vulnerabilities.....	108
Vulnerability Categories	108
Location of Privacy Vulnerabilities	109
National Vulnerability Database and Common Vulnerability Scoring System	110
4.7 Key Terms and Review Questions.....	114
Key Terms	114
Review Questions	115
4.8 References	116
Part III Technical Security Controls for Privacy	117
Chapter 5: System Access	118
5.1 System Access Concepts	119
Privileges.....	119
System Access Functions.....	120
Privacy Considerations for System Access.....	121

5.2	Authorization	122
	Privacy Authorization	123
5.3	User Authentication	124
	Means of Authentication	125
	Multifactor Authentication.....	126
	A Model for Electronic User Authentication.....	127
5.4	Access Control	129
	Subjects, Objects, and Access Rights.....	130
	Access Control Policies	131
	Discretionary Access Control.....	131
	Role-Based Access Control.....	133
	Attribute-Based Access Control	135
5.5	Identity and Access Management.....	140
	IAM Architecture	140
	Federated Identity Management.....	142
5.6	Key Terms and Review Questions.....	144
	Key Terms	144
	Review Questions	145
5.7	Reference	145
Chapter 6: Malicious Software and Intruders		146
6.1	Malware Protection Activities.....	147
	Types of Malware	147
	The Nature of the Malware Threat	149
	Practical Malware Protection.....	150
6.2	Malware Protection Software	153
	Capabilities of Malware Protection Software.....	153
	Managing Malware Protection Software.....	154

6.3	Firewalls.....	155
	Firewall Characteristics.....	155
	Types of Firewalls.....	156
	Next-Generation Firewalls	163
	DMZ Networks.....	164
	The Modern IT Perimeter	165
6.4	Intrusion Detection	166
	Basic Intrusion Detection Principles	167
	Approaches to Intrusion Detection	167
	Host-Based Intrusion Detection Techniques	169
	Network-Based Intrusion Detection Systems.....	169
	IDS Best Practices	171
6.5	Key Terms and Review Questions.....	172
	Key Terms	172
	Review Questions	173
6.6	References	174
Part IV Privacy Enhancing Technologies		175
Chapter 7: Privacy in Databases		176
7.1	Basic Concepts.....	178
	Personal Data Attributes.....	179
	Types of Data Files.....	180
7.2	Re-Identification Attacks.....	183
	Types of Attacks.....	184
	Potential Attackers.....	186
	Disclosure Risks.....	186
	Applicability to Privacy Threats.....	187
7.3	De-Identification of Direct Identifiers.....	188
	Anonymization	189
	Pseudonymization.....	189

7.4	De-Identification of Quasi-Identifiers in Microdata Files	190
	Privacy-Preserving Data Publishing.....	192
	Disclosure Risk Versus Data Utility	193
	PPDP Techniques	194
7.5	<i>K</i> -Anonymity, <i>L</i> -Diversity, and <i>T</i> -Closeness.....	196
	<i>K</i> -Anonymity	196
	<i>L</i> -Diversity	198
	<i>T</i> -Closeness.....	199
7.6	Summary Table Protection	199
	Frequency Tables.....	200
	Magnitude Tables.....	203
7.7	Privacy in Queryable Databases	204
	Privacy Threats	205
	Protecting Queryable Databases	206
7.8	Key Terms and Review Questions.....	211
	Key Terms	211
	Review Questions	212
7.9	References	212
	Chapter 8: Online Privacy	214
8.1	The Online Ecosystem for Personal Data.....	215
8.2	Web Security and Privacy	217
	Web Server Security and Privacy.....	218
	Web Application Security and Privacy.....	219
	Web Browser Security and Privacy.....	222
8.3	Mobile App Security	224
	Mobile Ecosystem.....	224
	Mobile Device Vulnerabilities	225
	BYOD Policies.....	227
	Mobile Application Vetting	229
	Resources for Mobile Device Security.....	230

8.4	Online Privacy Threats.....	231
	Web Application Privacy	231
	Mobile App Privacy.....	232
8.5	Online Privacy Requirements	234
	Online Privacy Principles	234
	Online Privacy Framework.....	236
	Simplified Consumer Choice	241
	Transparency of Data Practices	241
8.6	Privacy Notices.....	242
	Notice Requirements	243
	Notice Content.....	243
	Notice Structure	246
	Mobile App Privacy Notices.....	246
	Privacy Notice Design Space	248
8.7	Tracking	250
	Cookies	250
	Other Tracking Technologies.....	253
	Do Not Track	254
8.8	Key Terms and Review Questions.....	254
	Key Terms	254
	Review Questions	255
8.9	References	255
Chapter 9: Other PET Topics		258
9.1	Data Loss Prevention	258
	Data Classification and Identification	259
	Data States	260
	DLP for Email	262
	DLP Model	263

9.2	The Internet of Things	266
	Things on the Internet of Things	266
	Components of IoT-Enabled Things	266
	IoT and Cloud Context.....	267
9.3	IoT Security	270
	IoT Device Capabilities	270
	Security Challenges of the IoT Ecosystem	271
	IoT Security Objectives.....	273
9.4	IoT Privacy.....	274
	An IoT Model.....	275
	Privacy Engineering Objectives and Risks.....	276
	Challenges for Organizations.....	278
9.5	Cloud Computing	280
	Cloud Computing Elements.....	280
	Threats for Cloud Service Users.....	284
9.6	Cloud Privacy	285
	Data Collection	286
	Storage	287
	Sharing and Processing.....	290
	Deletion.....	290
9.7	Key Terms and Review Questions.....	290
	Key Terms	290
	Review Questions	291
9.8	References	291
	Part V Information Privacy Management	293
	Chapter 10: Information Privacy Governance and Management	294
10.1	Information Security Governance.....	295
	Information Security Management System.....	295
	Information Security Governance Concepts.....	295

Security Governance Components.....	298
Integration with Enterprise Architecture.....	303
Policies and Guidance	307
10.2 Information Privacy Governance.....	308
Information Privacy Roles.....	308
The Privacy Program Plan	312
10.3 Information Privacy Management	315
Key Areas of Privacy Management.....	316
Privacy Planning	317
Privacy Policy.....	319
10.4 OASIS Privacy Management Reference Model.....	322
Privacy Management Reference Model and Methodology (PMRM).....	322
Privacy by Design Documentation for Software Engineers	328
10.5 Key Terms and Review Questions.....	331
Key Terms	331
Review Questions	331
10.6 References	332
Chapter 11: Risk Management and Privacy Impact Assessment	334
11.1 Risk Assessment.....	335
Risk Assessment Process.....	335
Risk Assessment Challenges.....	339
Quantitative Risk Assessment	340
Qualitative Risk Assessment.....	342
11.2 Risk Management.....	346
NIST Risk Management Framework.....	347
ISO 27005: <i>Information Security Risk Management</i>	348
Risk Evaluation.....	351
Risk Treatment	352

11.3	Privacy Risk Assessment	353
	Privacy Impact	356
	Likelihood.....	361
	Assessing Privacy Risk	363
11.4	Privacy Impact Assessment	365
	Privacy Threshold Analysis	365
	Preparing for a PIA.....	366
	Identify PII Information Flows	367
	Identify Potential User Behavior	367
	Determine Relevant Privacy Safeguarding Requirements	368
	Assess Privacy Risk.....	368
	Determine Risk Treatment.....	368
	The PIA Report.....	369
	Implement Risk Treatment	370
	Review/Audit Implementation.....	370
	Examples	371
11.5	Key Terms and Review Questions.....	371
	Key Terms	371
	Review Questions	372
11.6	References	372
Chapter 12: Privacy Awareness, Training, and Education		374
12.1	Information Privacy Awareness	376
	Awareness Topics	377
	Awareness Program Communication Materials.....	378
	Awareness Program Evaluation	379
12.2	Privacy Training and Education	380
	Cybersecurity Essentials.....	380
	Role-Based Training.....	381
	Education and Certification	383

12.3	Acceptable Use Policies.....	384
	Information Security Acceptable Use Policy	384
	PII Acceptable Use Policy.....	386
12.4	Key Terms and Review Questions.....	386
	Key Terms	386
	Review Questions	387
12.5	References	387
Chapter 13: Event Monitoring, Auditing, and Incident Response		388
13.1	Event Monitoring	388
	Security Event Logging.....	389
	Security Event Management.....	391
	Event Logging Related to PII	392
13.2	Information Security Auditing.....	393
	Data to Collect for Auditing.....	394
	Internal and External Audits.....	395
	Security Audit Controls	396
13.3	Information Privacy Auditing	398
	Privacy Audit Checklist	398
	Privacy Controls.....	400
13.4	Privacy Incident Management and Response.....	401
	Objectives of Privacy Incident Management	401
	Privacy Incident Response Team.....	402
	Preparing for Privacy Incident Response	403
	Detection and Analysis	405
	Containment, Eradication, and Recovery	406
	Notification to Affected Individuals	407
	Post-Incident Activity.....	408

13.5	Key Terms and Review Questions.....	409
	Key Terms	409
	Review Questions	410
13.6	References	410
Part VI Legal and Regulatory Requirements		411
Chapter 14: The EU General Data Protection Regulation		412
14.1	Key Roles and Terms in the GDPR.....	413
14.2	Structure of the GDPR.....	415
14.3	GDPR Objectives and Scope	417
	Objectives	417
	Scope of the GDPR	418
14.4	GDPR Principles.....	420
	Fairness.....	421
	Lawful.....	422
	Transparency.....	423
14.5	Restrictions on Certain Types of Personal Data.....	423
	Children’s Personal Data.....	423
	Special Categories of Personal Data	424
14.6	Rights of the Data Subject	426
14.7	Controller, Processor, and Data Protection Officer	428
	Data Protection by Design and Default.....	428
	Records of Processing Activities	429
	Security of Processing	431
	Data Protection Officer	431
14.8	Data Protection Impact Assessment.....	433
	Risk and High Risk.....	433
	Determining Whether a DPIA Is Needed.....	434
	DPIA Process.....	436

GDPR Requirements.....	438
Criteria for an Acceptable DPIA.....	439
14.9 Key Terms and Review Questions.....	441
Key Terms	441
Review Questions	441
14.10 References	442
Chapter 15: U.S. Privacy Laws	444
15.1 A Survey of Federal U.S. Privacy Laws.....	445
15.2 Health Insurance Portability and Accountability Act.....	449
HIPAA Overview	449
HIPAA Privacy Rule.....	450
15.3 Health Information Technology for Economic and Clinical Health Act.....	456
Breach Notification	456
Encryption of PHI.....	457
Data Destruction	459
15.4 Children’s Online Privacy Protection Act.....	460
General Provisions.....	460
The COPPA Final Rule	461
15.5 California Consumer Privacy Act	462
Basic Concepts.....	462
Rights of Consumers	466
Comparison with the GDPR.....	468
15.6 Key Terms and Review Questions.....	470
Key Terms	470
Review Questions	470
15.7 References	471
Index	472
Appendix (Online Only): Answers to Review Questions	