

Contents

List of Figures	xi
List of Tables	xiii
Foreword	xv
Preface	xvii
Introduction	xix
I Understanding Security and Privacy	1
1 Why Privacy, Why This Book	3
Privacy as an Aspect of Data Security	4
Anatomy of an Attack	5
An Example Attack	6
Wondering When We'll Talk Privacy?	12
2 Privacy Theory	13
Real-World Privacy	14
What Does Privacy Mean?	14
Relevant Properties of Data	20
Access Control	25
3 Policy Enforcement	29
Concepts	30
Agents	34
Policy	40
Threat Models	42
Prevention	49
4 Online Privacy Concepts	55
Collection and Handling	57
Data Correctness	63
Policy Compliance	64

Contents

5 Threats to Privacy	67
Centralization	68
Linkability	71
Too Much Information	73
Leaky Channels	76
Secondary Uses	76
 II The Problem	 81
6 Design Principles	83
The Need for Secure Design Principles	84
Saltzer and Schroeder Secure Design Principles	86
Putting the Design Principles to Use	101
7 Deployment Environments	103
Internet Architecture	104
The Protocol Stack	105
The Domain Name System	109
World Wide Web Architecture	111
Addressing Objects on the Web	112
HTML, Architecturally	116
HTTP: Pulling Stuff from the Net	118
HTTP Cookies	123
Invading Your Privacy	127
How Online Advertising Erodes Privacy	128
The Internet as a Deployment Environment	138
8 Case Studies	139
Case Study #1: Centralization Unexpectedly Erodes Privacy	140
Case Study #2: Server Bug Undermines Opt-Out	154
Case Study #3: Client Design Undermines Opt-Out System	159
Case Study #4: Service Model Creates Privacy Holes	160
Case Study #5: The Struggle Between Convenience and Security	167
What We've Learned	171
 III The Cure	 173
9 Learning from Failure	175
Types of Failure	176
Contributors to Failure	179
Dealing with Failure	186
Minimizing the Impact of Failure	193

Contents

10 Why Opt-Out Systems Cannot Protect Privacy	199
Relevant Components	200
Systems for Data Collection	208
Policy, Policy, Policy	213
11 Earning Trust	215
The Business Case for Privacy	216
Policy	225
Practice	227
Maintaining Trust	237
12 Your First Assignment	239
Functional Requirements	242
Design	252
Deployment	258
Operation	261
Next Steps	262
References	263
Index	273