

# Contents

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

*Contents*

<b>5 Threats to Privacy</b>	<b>67</b>
Centralization . . . . .	68
Linkability . . . . .	71
Too Much Information . . . . .	73
Leaky Channels . . . . .	76
Secondary Uses . . . . .	76
 <b>II The Problem</b>	 <b>81</b>
<b>6 Design Principles</b>	<b>83</b>
The Need for Secure Design Principles . . . . .	84
Saltzer and Schroeder Secure Design Principles . . . . .	86
Putting the Design Principles to Use . . . . .	101
<b>7 Deployment Environments</b>	<b>103</b>
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
<b>8 Case Studies</b>	<b>139</b>
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
 <b>III The Cure</b>	 <b>173</b>
<b>9 Learning from Failure</b>	<b>175</b>
Types of Failure . . . . .	176
Contributors to Failure . . . . .	179
Dealing with Failure . . . . .	186
Minimizing the Impact of Failure . . . . .	193

*Contents*

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



<http://www.springer.com/978-1-893115-72-9>

Developing Trust

Online Privacy and Security

Curtin, M.

2002, XXI, 282 p., Softcover

ISBN: 978-1-893115-72-9

A product of Apress