# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>How This Book Is Organized</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>What's On the CD?</td>
<td>xv</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>About the Authors</td>
<td>xvii</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acknowledgements</td>
<td>xix</td>
</tr>
<tr>
<td></td>
<td>From Mark Merkow</td>
<td>xvii</td>
</tr>
<tr>
<td></td>
<td>From Laksh Raghavan</td>
<td>xviii</td>
</tr>
<tr>
<td>Chapter 1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Secure and Resilient</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Bad Design Choices Led to the Vulnerable Internet We Know Today</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>HTTP Has Its Problems, Too</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>Design Errors Continue Haunting Us Today</td>
<td>6</td>
</tr>
<tr>
<td>1.5</td>
<td>Requirements &amp; Design: The Keys to a Successful Software Project</td>
<td>7</td>
</tr>
<tr>
<td>1.6</td>
<td>How Design Flaws Play Out</td>
<td>10</td>
</tr>
<tr>
<td>1.6.1</td>
<td>DNS Vulnerability</td>
<td>10</td>
</tr>
<tr>
<td>1.6.2</td>
<td>The London Stock Exchange</td>
<td>10</td>
</tr>
<tr>
<td>1.6.3</td>
<td>Medical Equipment</td>
<td>11</td>
</tr>
<tr>
<td>1.6.4</td>
<td>Airbus A380</td>
<td>12</td>
</tr>
<tr>
<td>1.7</td>
<td>Solutions Are In Sight!</td>
<td>12</td>
</tr>
<tr>
<td>1.8</td>
<td>Notes</td>
<td>13</td>
</tr>
</tbody>
</table>
Chapter 2  Nonfunctional Requirements (NFRs) in Context 15

2.1  System Quality Requirements Engineering (SQUARE) 15
   2.1.1  Agree on Definitions 16
   2.1.2  Identify Assets and Security/Quality Goals 17
   2.1.3  Perform Risk Assessments 17
   2.1.4  Elicit Security Requirements 18
   2.1.5  Prioritize Requirements 20

2.2  Characteristics of Good Requirements 21
2.3  Summary 22
2.4  Notes 23

Chapter 3  Resilience and Quality Considerations for Application Software and the Application Runtime Environment 25

3.1  Relationships among Nonfunctional Requirements 26
3.2  Considerations for Developing NFRs for your Applications and Runtime Environment 26
3.3  Checking Your Work 51
3.4  Summary 52
3.5  Notes 52

Chapter 4  Security Requirements for Application Software 55

4.1  Security Control Types 55
4.2  Think Like an Attacker 56
4.3  Detailed Security Requirements 57
4.4  Identification Requirements 57
4.5  Authentication Requirements 61
4.6  Authorization Requirements 71
4.7  Security Auditing Requirements 79
4.8  Confidentiality Requirements 85
4.9  Integrity Requirements 91
4.10 Availability Requirements 96
4.11 Nonrepudiation Requirements 97
4.12 Immunity Requirements 99
4.13 Survivability Requirements 102
4.14 Systems Maintenance Security Requirements 104
4.15 Privacy Requirements 110
4.16 Summary 134
4.17 References 135
Chapter 5  Security Services for the Application Operating Environment  137

5.1 The Open Group Architecture Framework (TOGAF) 138
5.2 Standardizing Tools for an Enterprise Architecture  139
5.3 Security Technical Reference Model (TRM) 140
   5.3.1 Identification and Authentication 141
   5.3.2 System Entry Control 141
   5.3.3 Audit 142
   5.3.4 Access Control 143
   5.3.5 Nonrepudiation 143
   5.3.6 Security Management 144
   5.3.7 Trusted Recovery 144
   5.3.8 Encryption 144
   5.3.9 Trusted Communications 145

5.4 Summary 146
5.5 References 146

Chapter 6  Software Design Considerations for Security and Resilience  147

6.1 Design Issues 147
6.2 Architecture and Design Considerations 150
6.3 Special Security Design Considerations for Payment Applications on Mobile Communications Devices 154
6.4 Designing for Integrity 155
6.5 Architecture and Design Review Checklist 156
6.6 Summary 165
6.7 References 165

Chapter 7  Best Practices for Converting Requirements to Secure Software Designs  167

7.1 Secure Design Approach 167
7.2 Reusable Security APIs/Libraries 168
7.3 Security Frameworks 168
7.4 Establishing and Following Best Practices for Design 169
7.5 Security Requirements 169
7.6 Security Recommendations 170
7.7 What's an Attack Surface? 171
7.8 What Is Managed Code? 173
Chapter 8  Security Test Cases 177

8.1 Standardized Testing Policy 177
8.2 Security Test Cases 178
  8.2.1 Test Cases for Identification Requirements 179
  8.2.2 Test Cases for Authentication Requirements 181
8.3 Test Cases for Authorization Requirements 189
  8.3.1 Test Cases for Security Auditing Requirements 195
  8.3.2 Test Cases for Confidentiality Requirements 199
  8.3.3 Test Cases for Integrity Requirements 203
  8.3.4 Test Cases for Availability Requirements 206
  8.3.5 Test Cases for Nonrepudiation Requirements 207
  8.3.6 Test Cases for Immunity Requirements 209
  8.3.7 Test Cases for Survivability Requirements 210
  8.3.8 Test Cases for Systems Maintenance Security Requirements 212
8.4 Summary 215

Chapter 9  Testing Methods and Best Practices 217

9.1 Secure Testing Approach 217
9.2 OWASP’s Application Security Verification Standard (ASVS) 217
  9.2.1 Application Security Verification Levels 219
  9.2.2 Level 1—Automated Verification 220
  9.2.3 Level 2—Manual Verification 220
  9.2.4 Level 3—Design Verification 221
  9.2.5 Level 4—Internal Verification 222
  9.2.6 Security Testing Methods 224
9.3 Manual Source Code Review 224
9.4 Automated Source Code Analysis 225