FOREWORD BY
HOWARD SCHMIDT

CORE SOFTWARE SECURITY

SECURITY AT THE SOURCE

JAMES RANSOME
ANMOL MISRA

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

005.8
RAN

CORE SOFTWARE SECURITY

SECURITY AT THE SOURCE

Contents

Dedication v

Foreword by Hon. Howard A. Schmidt xiii

Preface xix

Acknowledgments xxiii

About the Authors xxv

Chapter 1 Introduction 1

1.1 The Importance and Relevance of Software Security 3
1.2 Software Security and the Software Development Lifecycle 6
1.3 Quality Versus Secure Code 10
1.4 The Three Most Important SDL Security Goals 11
1.5 Threat Modeling and Attack Surface Validation 13
1.6 Chapter Summary—What to Expect from This Book 15
References 16

Chapter 2 The Secure Development Lifecycle 19

2.1 Overcoming Challenges in Making Software Secure 20
2.2 Software Security Maturity Models 21
2.3 ISO/IEC 27034—Information Technology—Security Techniques—Application Security 23
2.4 Other Resources for SDL Best Practices 25

2.4.1 SAFECode 25
2.4.2 U.S. Department of Homeland Security Software Assurance Program 26
2.4.3 National Institute of Standards and Technology 27
2.4.4 MITRE Corporation Common Computer Vulnerabilities and Exposures 28
2.4.5 SANS Institute Top Cyber Security Risks 30
2.4.6 U.S. Department of Defense Cyber Security and Information Systems Information Analysis Center (CSIAC) 30
2.4.7 CERT, Bugtraq, and SecurityFocus 31
2.5 Critical Tools and Talent 31
2.5.1 The Tools 32
2.5.2 The Talent 34
2.6 Principles of Least Privilege 40
2.7 Privacy 41
2.8 The Importance of Metrics 42
2.9 Mapping the Security Development Lifecycle to the Software Development Lifecycle 45
2.10 Software Development Methodologies 50
2.10.1 Waterfall Development 51
2.10.2 Agile Development 53
2.3 Chapter Summary 56
References 57

Chapter 3 Security Assessment (A1): SDL Activities and Best Practices 61

3.1 Software Security Team Is Looped in Early 63
3.2 Software Security Hosts a Discovery Meeting 64
3.3 Software Security Team Creates an SDL Project Plan 66
3.4 Privacy Impact Assessment (PIA) Plan Initiated 66
3.5 Security Assessment (A1) Key Success Factors and Metrics 73
3.5.1 Key Success Factors 73
3.5.2 Deliverables 76
3.5.3 Metrics 78
3.6 Chapter Summary 79
References 79

Chapter 4 Architecture (A2): SDL Activities and Best Practices 81

4.1 A2 Policy Compliance Analysis 83
4.2 SDL Policy Assessment and Scoping 84
4.3 Threat Modeling/Architecture Security Analysis 84
4.3.1 Threat Modeling 84
4.3.2 Data Flow Diagrams 88
4.3.3 Architectural Threat Analysis and Ranking of Threats 95
4.3.4 Risk Mitigation 117
4.4 Open-Source Selection 124
4.5 Privacy Information Gathering and Analysis 124
4.6 Key Success Factors and Metrics 125
4.6.1 Key Success Factors 125
4.6.2 Deliverables 126
4.6.3 Metrics 127
4.7 Chapter Summary 128
References 129

Chapter 5 Design and Development (A3): SDL Activities and Best Practices 133

5.1 A3 Policy Compliance Analysis 135
5.2 Security Test Plan Composition 135
5.3 Threat Model Updating 146
5.4 Design Security Analysis and Review 146
5.5 Privacy Implementation Assessment 150
5.6 Key Success Factors and Metrics 154
5.6.1 Key Success Factors 154
5.6.2 Deliverables 156
5.6.3 Metrics 157
5.7 Chapter Summary 158
References 158

Chapter 6 Design and Development (A4): SDL Activities and Best Practices 161

6.1 A4 Policy Compliance Analysis 163
6.2 Security Test Case Execution 164
6.3 Code Review in the SDLC/SDL Process 168

6.4 Security Analysis Tools 174
6.4.1 Static Analysis 177
6.4.2 Dynamic Analysis 182
6.4.3 Fuzz Testing 185
6.4.4 Manual Code Review 188
6.5 Key Success Factors 192
6.6 Deliverables 193
6.7 Metrics 194
6.8 Chapter Summary 195
References 195

Chapter 7 Ship (A5): SDL Activities and Best Practices 199

7.1 A5 Policy Compliance Analysis 201
7.2 Vulnerability Scan 202
7.3 Penetration Testing 205
7.4 Open-Source Licensing Review 208
7.5 Final Security Review 212
7.6 Final Privacy Review 216
7.7 Key Success Factors 217
7.8 Deliverables 219
7.9 Metrics 221
7.10 Chapter Summary 221
References 223

Chapter 8 Post-Release Support (PRSA1–5) 225

8.1 Right-Sizing Your Software Security Group 227
8.1.1 The Right Organizational Location 227
8.1.2 The Right People 229
8.1.3 The Right Process 229
8.2 PRSA1: External Vulnerability Disclosure Response 232
8.2.1 Post-Release PSIRT Response 233
8.2.2 Post-Release Privacy Response 238
8.2.3 Optimizing Post-Release Third-Party Response 239
8.3 PRSA2: Third-Party Reviews 240
8.4 PRSA3: Post-Release Certifications 242
8.5 PRSA4: Internal Review for New Product Combinations or Cloud Deployments 243

8.6 PRSA5: Security Architectural Reviews and Tool-Based Assessments of Current, Legacy, and M&A Products and Solutions 243
8.6.1 Legacy Code 243
8.6.2 Mergers and Acquisitions (M&As) 247
8.7 Key Success Factors 248
8.8 Deliverables 251
8.9 Metrics 252
8.10 Chapter Summary 252
References 253

Chapter 9 Applying the SDL Framework to the Real World 255

9.0 Introduction 256
9.1 Build Software Securely 261
9.1.1 Produce Secure Code 264
9.1.2 Manual Code Review 269
9.1.3 Static Analysis 271
9.2 Determining the Right Activities for Each Project 275
9.2.1 The Seven Determining Questions 275
9.3 Architecture and Design 292
9.4 Testing 302
9.4.1 Functional Testing 303
9.4.2 Dynamic Testing 304
9.4.3 Attack and Penetration Testing 309
9.4.4 Independent Testing 311
9.5 Agile: Sprints 312
9.6 Key Success Factors and Metrics 317
9.6.1 Secure Coding Training Program 317
9.6.2 Secure Coding Frameworks (APIs) 318
9.6.3 Manual Code Review 318
9.6.4 Independent Code Review and Testing (by Experts or Third Parties) 318
9.6.5 Static Analysis 319
9.6.6 Risk Assessment Methodology 319
9.6.7 Integration of SDL with SDLC 319
9.6.8 Development of Architecture Talent 319
9.7 Metrics 320
9.8 Chapter Summary 321
References 323

Chapter 10 Pulling It All Together: Using the SDL to Prevent Real-World Threats 325
10.1 Strategic, Tactical, and User-Specific Software Attacks 326
10.1.1 Strategic Attacks 328
10.1.2 Tactical Attacks 338
10.1.3 User-Specific Attacks 339
10.2 Overcoming Organizational and Business Challenges with a Properly Designed, Managed, and Focused SDL 339
10.3 Software Security Organizational Realities and Leverage 340
10.4 Overcoming SDL Audit and Regulatory Challenges with Proper Governance Management 342
10.5 Future Predications for Software Security 343
10.5.1 The Bad News 343
10.5.2 The Good News 345
10.6 Conclusion 345
References 347

Appendix 351

Index 359