



Web Commerce Security Design and Development

Hadi Nahari
Ronald L. Krutz



WILEY

Wiley Publishing, Inc.



Contents

| | | |
|------------------|---|--------------|
| | Foreword by John Donahoe | xxi |
| | Foreword by Scott Thompson | xxiii |
| | Introduction | xxv |
| Part I | Overview of Commerce | 1 |
| Chapter 1 | Internet Era: E-Commerce | 3 |
| | Evolution of Commerce | 3 |
| | Hard vs. Digital Goods | 4 |
| | Payment | 5 |
| | Money | 6 |
| | Financial Networks | 6 |
| | ACH | 9 |
| | Card Processing | 10 |
| | Mobile Payment and Commerce | 14 |
| | Distributed Computing: Adding E to Commerce | 16 |
| | Client/Server | 17 |
| | Grid Computing | 18 |
| | Cloud Computing | 20 |
| | Shared Resources | 22 |
| | Dynamic Resource Allocation | 22 |
| | Physical Abstraction | 23 |
| | Utility Model | 23 |
| | Self Service | 23 |
| | SLA-Driven Management | 24 |
| | Automation | 24 |
| | Self-Healing | 24 |
| | Service Orientation | 25 |
| | Multi-Tenancy | 25 |

| | |
|---|-----------|
| Cloud Security | 25 |
| Architecture Review | 25 |
| Centralized Authentication | 26 |
| Single Sign-On and Delegation | 26 |
| Role-Based Access Control | 27 |
| Credential Store | 27 |
| Secure Communication and Storage | 28 |
| Isolated Management | 28 |
| Regulatory Compliance | 28 |
| Distributed Trust | 28 |
| Freshness | 29 |
| Trust | 29 |
| Secure Isolation | 29 |
| Authorization | 31 |
| Threats | 32 |
| Operational Aspects | 35 |
| Governance | 36 |
| Summary | 39 |
| Notes | 39 |
| Chapter 2 Mobile Commerce | 41 |
| Consumer Electronics Devices | 42 |
| Mobile Phone and M-Commerce | 42 |
| Landscape | 42 |
| M- vs. E-commerce | 46 |
| Mobile Hardware | 46 |
| Device Manufacturer | 47 |
| Operating System | 48 |
| Stack | 49 |
| Application Model | 49 |
| State of Mobile | 52 |
| Mobile Technologies: Mosquito on Steroids | 54 |
| Carrier Networks | 54 |
| Stacks | 57 |
| Java Micro Edition | 57 |
| Android | 61 |
| BlackBerry | 67 |
| iPhone | 68 |
| Symbian | 73 |
| Other Stacks | 74 |
| Summary | 75 |
| Notes | 75 |
| Chapter 3 Important “Ilities” in Web Commerce Security | 77 |
| Confidentiality, Integrity, and Availability | 77 |
| Confidentiality | 77 |
| Integrity | 78 |
| Availability | 79 |

| | | |
|---|---------------------------------|------------|
| Extensibility | 80 | |
| Black Box Extensibility | 81 | |
| White Box Extensibility (Open Box) | 82 | |
| White Box Extensibility (Glass Box) | 82 | |
| Gray Box Extensibility | 83 | |
| Fault Tolerability | 84 | |
| High Availability | 85 | |
| Telecommunications Network Fault Tolerance | 86 | |
| Interoperability | 86 | |
| Additional Interoperability Standards | 87 | |
| Testing for Interoperability | 87 | |
| Maintainability | 88 | |
| Manageability | 89 | |
| Modularity | 89 | |
| Monitorability | 90 | |
| Intrusion Detection | 91 | |
| Penetration Testing | 92 | |
| Violation Analysis | 92 | |
| Operability | 93 | |
| Protection of Resources and Privileged Entities | 94 | |
| Categories of Web Commerce Operability Controls | 94 | |
| Portability | 95 | |
| Predictability | 96 | |
| Reliability | 97 | |
| Ubiquity | 98 | |
| Usability | 99 | |
| Scalability | 99 | |
| Accountability | 101 | |
| Audit Ability | 101 | |
| Traceability | 103 | |
| Summary | 104 | |
| Notes | 105 | |
| Part II | E-Commerce Security | 107 |
| Chapter 4 | E-Commerce Basics | 109 |
| | Why E-Commerce Security Matters | 109 |
| | What Makes a System Secure | 110 |
| | Risk-Driven Security | 112 |
| | Security and Usability | 114 |
| | Usability of Passwords | 114 |
| | Practical Notes | 115 |
| | Scalable Security | 116 |
| | Securing Your Transactions | 117 |
| | How Secure Is Secure? | 118 |
| | Summary | 118 |
| | Notes | 118 |

| | | |
|------------------|--|------------|
| Chapter 5 | Building Blocks: Your Tools | 119 |
| | Cryptography | 119 |
| | The Role of Cryptography | 119 |
| | Symmetric Cryptosystems | 120 |
| | Stream Ciphers | 120 |
| | Block Ciphers | 121 |
| | Initialization Vector | 123 |
| | Some Classical Ciphers | 123 |
| | Symmetric Key Cryptography Fundamentals | 127 |
| | Asymmetric Cryptosystems | 131 |
| | One-Way Functions | 132 |
| | Public Key Algorithms | 132 |
| | Public Key Cryptosystems Algorithm Categories | 135 |
| | Asymmetric and Symmetric Key Length Strength Comparisons | 135 |
| | Digital Signatures | 136 |
| | Message Digest | 136 |
| | Hash Function Characteristics | 138 |
| | Digital Signature Standard and Secure Hash Standard | 138 |
| | Hashed Message Authentication Code | 139 |
| | Random Number Generation | 140 |
| | NIST SP 800-90 | 140 |
| | Other PRN Generators | 141 |
| | FIPS 140-2 | 141 |
| | Public Key Certification Systems-Digital Certificates | 142 |
| | Public Key Infrastructure | 142 |
| | Digital Certificates | 143 |
| | Directories and X.500 | 143 |
| | The Lightweight Directory Access Protocol | 144 |
| | X.509 Certificates | 144 |
| | Certificate Revocation Lists | 145 |
| | Certificate Extensions | 146 |
| | Key Management | 147 |
| | Distributed versus Centralized Key Management | 149 |
| | Data Protection | 149 |
| | Data Loss Prevention | 150 |
| | Database Security | 150 |
| | Access Control | 152 |
| | Controls | 152 |
| | Models for Controlling Access | 153 |
| | Mandatory Access Control | 153 |
| | Discretionary Access Control | 154 |
| | Non-Discretionary Access Control | 154 |
| | System Hardening | 155 |
| | Service Level Security | 155 |
| | Web Servers | 155 |

| | |
|---|------------|
| Web Server Security | 156 |
| Web Services | 163 |
| Web Applications | 166 |
| Host Level Security | 170 |
| Operating Systems | 170 |
| Browser Clients | 172 |
| Native Client | 173 |
| Network Security | 173 |
| Firewalls | 174 |
| Protocols | 176 |
| E-Mail | 184 |
| Malware Issues | 186 |
| Anti-Phishing | 189 |
| Network Utility Programs | 190 |
| Summary | 191 |
| Notes | 191 |
| Chapter 6 System Components: What You Should Implement | 193 |
| Authentication | 193 |
| User Authentication | 193 |
| Passwords | 194 |
| Biometrics | 196 |
| Network Authentication | 197 |
| Device Authentication | 200 |
| API Authentication | 201 |
| HTTP Basic Authentication | 201 |
| HTTP Digest Access Authentication | 201 |
| Microsoft Windows Challenge/Response (NTLM) | |
| Authentication | 202 |
| AuthSub | 203 |
| The OAuth 1.0 Protocol | 203 |
| Process Authentication | 204 |
| Authorization | 205 |
| Non-Repudiation | 206 |
| Privacy | 206 |
| Privacy Policy | 207 |
| Privacy-Related Legislation and Guidelines | 208 |
| European Union Principles | 208 |
| Health Care-Related Privacy Issues | 209 |
| The Platform for Privacy Preferences | 210 |
| Electronic Monitoring | 211 |
| Information Security | 213 |
| Security Management Concepts | 213 |
| System Security Life Cycle | 213 |
| Confidentiality, Integrity, and Availability | 214 |
| Layered Security Architecture | 214 |
| Security Controls | 215 |

| | |
|--|------------|
| Data and Information Classification | 215 |
| Information Classification Benefits | 216 |
| Information Classification Concepts | 216 |
| Classification Terms | 217 |
| Classification Criteria | 218 |
| Information Classification Procedures | 218 |
| Distribution of Classified Information | 219 |
| Information Classification Roles | 219 |
| Data Categorization | 222 |
| Bell-LaPadula Model | 223 |
| System and Data Audit | 224 |
| Syslog | 226 |
| SIEM | 228 |
| Defense in Depth | 229 |
| Principle of Least Privilege | 232 |
| Trust | 234 |
| Isolation | 235 |
| Virtualization | 236 |
| Sandbox | 236 |
| IPSec Domain Isolation | 236 |
| Security Policy | 237 |
| Senior Management Policy Statement | 238 |
| Advisory Policies | 238 |
| Regulatory Policies | 238 |
| Informative Policies | 238 |
| NIST Policy Categories | 238 |
| Communications Security | 239 |
| Inter-Network Security | 239 |
| Homogenous Networks | 241 |
| Heterogeneous networks | 242 |
| Summary | 243 |
| Notes | 243 |
| Chapter 7 Trust but Verify: Checking Security | 245 |
| Tools to Verify Security | 246 |
| Vulnerability Assessment and Threat Analysis | 247 |
| Intrusion Detection and Prevention Using Snort | 249 |
| Network Scanning Using Nmap | 251 |
| Web Application Survey | 252 |
| Lynx | 252 |
| Wget | 253 |
| Teleport Pro | 254 |
| BlackWidow | 255 |
| BrownRecluse Pro | 255 |
| Vulnerability Scanning | 257 |
| Nessus | 257 |
| Nikto | 258 |
| Wireshark | 259 |

| | |
|--|------------|
| Penetration Testing | 260 |
| Metasploit | 260 |
| Aircrack-ng | 261 |
| Wireless Reconnaissance | 262 |
| NetStumbler | 262 |
| Kismet | 263 |
| AirMagnet Wi-Fi Analyzer | 264 |
| Summary | 266 |
| Notes | 266 |
| Chapter 8 Threats and Attacks: What Your Adversaries Do | 267 |
| Basic Definitions | 268 |
| Target | 268 |
| Threat | 269 |
| Threat Modeling | 269 |
| Attack | 269 |
| Attack Tree | 269 |
| Zero-Day Attack | 270 |
| Control | 270 |
| Same-Origin Policy | 270 |
| Common Web Commerce Attacks | 271 |
| Broken Authentication and Session Management Attack | 271 |
| Control | 272 |
| Cross-Site Request Forgery Attack | 272 |
| Control | 275 |
| Cross-Site Scripting Attack | 276 |
| Stored or Persistent XSS | 276 |
| Reflected or Non-Persistent XSS | 277 |
| DOM-Based XSS | 277 |
| Control | 278 |
| DNS Hijacking Attack | 280 |
| Control | 281 |
| Failure to Restrict URL Access Attack | 281 |
| Control | 281 |
| Injection Flaws | 282 |
| Attacks | 282 |
| Control | 285 |
| Insufficient Transport Layer Protection Attack | 285 |
| Control | 285 |
| Insecure Cryptographic Storage Attack | 286 |
| Control | 286 |
| Insecure Direct Object Reference Attack | 287 |
| Control | 287 |
| Phishing and Spamming Attack | 287 |
| Control | 288 |
| Rootkits and Their Related Attacks | 288 |
| Control | 288 |

| | |
|--|------------|
| Security Misconfiguration Attack | 289 |
| Control | 289 |
| Unvalidated Redirects and Forwards Attack | 289 |
| Control | 290 |
| Summary | 290 |
| Notes | 290 |
| Chapter 9 Certification: Your Assurance | 293 |
| Certification and Accreditation | 293 |
| The Certification Process | 294 |
| Security Control Assessment | 294 |
| Standards and Related Guidance | 296 |
| Trusted Computer System Evaluation Criteria | 296 |
| Common Criteria ISO/IEC 15408 | 297 |
| Defense Information Assurance Certification and Accreditation Process | 297 |
| The DIACAP Phases | 298 |
| Office of Management and Budget Circular A-130 | 299 |
| The National Information Assurance Certification and Accreditation Process | 300 |
| NIACAP Accreditation Types | 302 |
| The Four Phases of NIACAP | 302 |
| Roles of NIACAP | 303 |
| Federal Information Security Management Act | 303 |
| Federal Information Technology Security Assessment Framework | 303 |
| FIPS 199 | 304 |
| FIPS 200 | 305 |
| Additional Guidance | 306 |
| Related Standards Bodies and Organizations | 306 |
| Jericho Forum | 307 |
| The Distributed Management Task Force | 307 |
| The DMTF Open Virtualization Format | 307 |
| International Organization for Standardization/International Electrotechnical Commission | 308 |
| ISO 27001 | 308 |
| ISO 27002 | 309 |
| ISO 27004 | 310 |
| ISO 27006 | 310 |
| ISO/IEC 29361, ISO/IEC 29362, and ISO/IEC 29363 Standards | 310 |
| Distributed Application Platforms and Services | 311 |
| The European Telecommunications Standards Institute | 311 |
| Storage Networking Industry Association | 311 |

| | |
|---|-----|
| The Open Web Application Security Project | 312 |
| OWASP Top Ten Project | 313 |
| OWASP Development Guide | 313 |
| NIST SP 800-30 | 314 |
| Risk Assessment | 315 |
| Risk Mitigation | 316 |
| Evaluation and Assessment | 316 |
| Residual Risk | 316 |
| Certification Laboratories | 316 |
| The Software Engineering Center Software Assurance Laboratory | 317 |
| SAIC | 317 |
| ICSA Labs | 317 |
| The Systems Security Engineering Capability Maturity Model | 318 |
| Value of Certification | 321 |
| When It Matters | 322 |
| When It Does Not | 322 |
| Certification Types | 323 |
| Common Criteria | 323 |
| MasterCard CAST | 323 |
| EMV | 324 |
| VSDC – VISA | 324 |
| M/Chip | 325 |
| GlobalPlatform Composition Model | 325 |
| Other Evaluation Criteria | 325 |
| NSA | 327 |
| The IAM Process | 328 |
| FIPS 140 Certification and NIST | 328 |
| Summary | 329 |
| Notes | 330 |

| | |
|--|------------|
| Appendix A Computing Fundamentals | 331 |
| Introduction | 331 |
| Hardware | 334 |
| Central Processing Unit | 334 |
| Instruction Execution Cycle | 338 |
| A Bit about Bytes | 345 |
| Memory and Storage | 345 |
| Input and Output | 350 |
| Popular Architectures | 351 |
| ARM | 351 |
| MIPS | 352 |
| PowerPC | 353 |
| X86 | 353 |
| XScale | 354 |

| | |
|---|------------|
| Software | 355 |
| Underware | 357 |
| Firmware | 357 |
| Virtualization | 357 |
| Operating System | 359 |
| Middleware | 362 |
| Applications | 363 |
| Programming Languages | 363 |
| Summary | 364 |
| Appendix B Standardization and Regulatory Bodies | 365 |
| ANSI | 366 |
| COBIT | 366 |
| COSO | 367 |
| CSA | 367 |
| Ecma | 368 |
| ETSI | 368 |
| FIPS | 369 |
| GlobalPlatform | 370 |
| IANA | 371 |
| IEC | 372 |
| IETF | 372 |
| ISO | 372 |
| Kantara | 373 |
| NIST | 373 |
| OASIS | 376 |
| OAuth | 377 |
| OpenID | 377 |
| OpenSAF | 378 |
| PCI | 379 |
| SAF | 380 |
| SOX | 380 |
| The Open Group | 381 |
| W3C | 382 |
| WASC | 382 |
| Notes | 383 |
| Appendix C Glossary of Terms | 385 |
| Appendix D Bibliography | 449 |
| Index | 457 |