

Contents

| | |
|--|-----------|
| Preface | ix |
| CHAPTER 1 – Introduction | 1 |
| 1.1 Attacks and Attackers | 2 |
| 1.2 Security | 4 |
| 1.3 Security Management | 4 |
| 1.4 Risk and Threat Analysis | 9 |
| CHAPTER 2 – Foundations of Computer Security | 17 |
| 2.1 Definitions | 18 |
| 2.2 The Fundamental Dilemma of Computer Security | 25 |
| 2.3 Data vs Information | 26 |
| 2.4 Principles of Computer Security | 27 |
| 2.5 The Layer Below | 31 |
| CHAPTER 3 – Identification and Authentication | 35 |
| 3.1 Username and Password | 36 |
| 3.2 Managing Passwords | 37 |
| 3.3 Choosing Passwords | 38 |
| 3.4 Spoofing Attacks | 40 |
| 3.5 Protecting the Password File | 41 |
| 3.6 Single Sign-on | 43 |
| 3.7 Alternative Approaches | 44 |
| CHAPTER 4 – Access Control | 51 |
| 4.1 Background | 52 |
| 4.2 Authentication and Authorization | 52 |
| 4.3 Access Operations | 54 |
| 4.4 Ownership | 57 |
| 4.5 Access Control Structures | 57 |
| 4.6 Intermediate Controls | 60 |
| 4.7 Partial Orderings | 64 |
| CHAPTER 5 – Reference Monitors | 71 |
| 5.1 Introduction | 72 |
| 5.2 Operating System Integrity | 74 |
| 5.3 Hardware Security Features | 75 |
| 5.4 Protecting Memory | 83 |

| | |
|--|------------|
| CHAPTER 6 – Unix Security | 91 |
| 6.1 Introduction | 92 |
| 6.2 Principals | 93 |
| 6.3 Subjects | 95 |
| 6.4 Objects | 97 |
| 6.5 Access Control | 101 |
| 6.6 Instances of General Security Principles | 104 |
| 6.7 Management Issues | 110 |
| CHAPTER 7 – Windows 2000 Security | 115 |
| 7.1 Introduction | 116 |
| 7.2 Access Control – Components | 119 |
| 7.3 Access Decisions | 127 |
| 7.4 Restricted Context | 132 |
| 7.5 Administration | 134 |
| CHAPTER 8 – Bell–LaPadula Model | 139 |
| 8.1 State Machine Models | 140 |
| 8.2 The Bell–LaPadula Model | 140 |
| 8.3 The Multics Interpretation of BLP | 146 |
| CHAPTER 9 – Security Models | 153 |
| 9.1 The Biba Model | 154 |
| 9.2 The Chinese Wall Model | 155 |
| 9.3 The Clark–Wilson Model | 157 |
| 9.4 The Harrison–Ruzzo–Ullman Model | 159 |
| 9.5 Information Flow Models | 162 |
| 9.6 Execution Monitors | 164 |
| CHAPTER 10 – Security Evaluation | 169 |
| 10.1 Introduction | 170 |
| 10.2 The Orange Book | 173 |
| 10.3 The Rainbow Series | 177 |
| 10.4 Information Technology Security Evaluation Criteria | 177 |
| 10.5 The Federal Criteria | 178 |
| 10.6 The Common Criteria | 179 |
| 10.7 Quality Standards | 182 |
| 10.8 An Effort Well Spent? | 182 |
| CHAPTER 11 – Cryptography | 185 |
| 11.1 Introduction | 186 |
| 11.2 Modular Arithmetic | 189 |
| 11.3 Integrity Check Functions | 191 |
| 11.4 Digital Signatures | 194 |
| 11.5 Encryption | 198 |

| | | |
|---|--------------------------------------|------------|
| 11.6 | Strength of Mechanisms | 205 |
| 11.7 | Performance | 207 |
| CHAPTER 12 – Authentication in Distributed Systems | | 211 |
| 12.1 | Introduction | 212 |
| 12.2 | Key Establishment and Authentication | 212 |
| 12.3 | Key Establishment Protocols | 215 |
| 12.4 | Kerberos | 219 |
| 12.5 | Public Key Infrastructures | 224 |
| 12.6 | Trusted Computing–Attestation | 229 |
| CHAPTER 13 – Network Security | | 233 |
| 13.1 | Introduction | 234 |
| 13.2 | Protocol Design Principles | 237 |
| 13.3 | IP Security | 239 |
| 13.4 | SSL/TLS | 243 |
| 13.5 | DNS | 247 |
| 13.6 | Firewalls | 247 |
| 13.7 | Intrusion Detection | 251 |
| CHAPTER 14 – Software Security | | 257 |
| 14.1 | Introduction | 258 |
| 14.2 | Characters and Numbers | 259 |
| 14.3 | Canonical Representations | 263 |
| 14.4 | Memory Management | 264 |
| 14.5 | Data and Code | 271 |
| 14.6 | Race conditions | 274 |
| 14.7 | Defenses | 275 |
| CHAPTER 15 – New Access Control Paradigms | | 283 |
| 15.1 | Introduction | 284 |
| 15.2 | Code-based Access Control | 286 |
| 15.3 | Java Security | 290 |
| 15.4 | .NET Security Framework | 295 |
| 15.5 | Cookies | 299 |
| 15.6 | SPKI | 301 |
| 15.7 | Trust Management | 302 |
| 15.8 | Digital Rights Management | 304 |
| CHAPTER 16 – Mobility | | 307 |
| 16.1 | Introduction | 308 |
| 16.2 | GSM | 308 |
| 16.3 | UMTS | 313 |
| 16.4 | Mobile IPv6 Security | 315 |

| | | |
|---------------------------------------|---------------------------------------|------------|
| 16.5 | WLAN | 320 |
| 16.6 | Bluetooth | 324 |
| CHAPTER 17 – Database Security | | 327 |
| 17.1 | Introduction | 328 |
| 17.2 | Relational Databases | 330 |
| 17.3 | Access Control | 334 |
| 17.4 | Statistical Database Security | 339 |
| 17.5 | Integration with the Operating System | 344 |
| 17.6 | Privacy | 346 |
| Bibliography | | 349 |
| Index | | 361 |