

Introduction to Computer Security

Matt Bishop



Addison-Wesley

Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

| | |
|--|------------|
| Preface | xxv |
| Goals | xxvi |
| Philosophy | xxvii |
| Organization | xxix |
| Differences Between this Book and <i>Computer Security</i> : | |
| <i>Art and Science</i> | xxx |
| Special Acknowledgment | xxxii |
| Acknowledgments | xxxii |
| | |
| Chapter 1 An Overview of Computer Security | 1 |
| 1.1 The Basic Components | 1 |
| 1.1.1 Confidentiality | 2 |
| 1.1.2 Integrity | 3 |
| 1.1.3 Availability | 4 |
| 1.2 Threats | 4 |
| 1.3 Policy and Mechanism | 7 |
| 1.3.1 Goals of Security | 8 |
| 1.4 Assumptions and Trust | 9 |
| 1.5 Assurance | 10 |
| 1.5.1 Specification | 11 |
| 1.5.2 Design | 12 |
| 1.5.3 Implementation | 12 |
| 1.6 Operational Issues | 14 |
| 1.6.1 Cost-Benefit Analysis | 14 |
| 1.6.2 Risk Analysis | 15 |
| 1.6.3 Laws and Customs | 16 |
| 1.7 Human Issues | 17 |
| 1.7.1 Organizational Problems | 18 |
| 1.7.2 People Problems | 19 |
| 1.8 Tying It All Together | 20 |
| 1.9 Summary | 21 |
| 1.10 Further Reading | 22 |
| 1.11 Exercises | 22 |

| | |
|---|-----------|
| Chapter 2 Access Control Matrix | 27 |
| 2.1 Protection State | 27 |
| 2.2 Access Control Matrix Model | 28 |
| 2.3 Protection State Transitions | 31 |
| 2.3.1 Conditional Commands | 33 |
| 2.4 Summary | 34 |
| 2.5 Further Reading | 35 |
| 2.6 Exercises | 35 |
| Chapter 3 Foundational Results | 37 |
| 3.1 The General Question | 37 |
| 3.2 Basic Results | 38 |
| 3.3 Summary | 43 |
| 3.4 Further Reading | 43 |
| 3.5 Exercises | 44 |
| Chapter 4 Security Policies | 45 |
| 4.1 Security Policies | 45 |
| 4.2 Types of Security Policies | 49 |
| 4.3 The Role of Trust | 51 |
| 4.4 Types of Access Control | 53 |
| 4.5 Example: Academic Computer Security Policy | 54 |
| 4.5.1 General University Policy | 55 |
| 4.5.2 Electronic Mail Policy | 55 |
| 4.5.2.1 <i>The Electronic Mail Policy Summary</i> | 56 |
| 4.5.2.2 <i>The Full Policy</i> | 56 |
| 4.5.2.3 <i>Implementation at UC Davis</i> | 57 |
| 4.6 Summary | 58 |
| 4.7 Further Reading | 58 |
| 4.8 Exercises | 59 |
| Chapter 5 Confidentiality Policies | 61 |
| 5.1 Goals of Confidentiality Policies | 61 |
| 5.2 The Bell-LaPadula Model | 62 |
| 5.2.1 Informal Description | 62 |
| 5.2.2 Example: The Data General B2 UNIX System | 66 |
| 5.2.2.1 <i>Assigning MAC Labels</i> | 66 |
| 5.2.2.2 <i>Using MAC Labels</i> | 69 |
| 5.3 Summary | 70 |
| 5.4 Further Reading | 70 |
| 5.5 Exercises | 71 |

| | |
|--|-----------|
| Chapter 6 Integrity Policies. | 73 |
| 6.1 Goals | 73 |
| 6.2 Biba Integrity Model | 75 |
| 6.3 Clark-Wilson Integrity Model | 76 |
| 6.3.1 The Model | 77 |
| 6.3.2 Comparison with the Requirements | 79 |
| 6.3.3 Comparison with Other Models | 80 |
| 6.4 Summary | 81 |
| 6.5 Further Reading | 81 |
| 6.6 Exercises | 82 |
| Chapter 7 Hybrid Policies. | 83 |
| 7.1 Chinese Wall Model | 83 |
| 7.1.1 Bell-LaPadula and Chinese Wall Models | 86 |
| 7.1.2 Clark-Wilson and Chinese Wall Models | 87 |
| 7.2 Clinical Information Systems Security Policy | 88 |
| 7.2.1 Bell-LaPadula and Clark-Wilson Models | 90 |
| 7.3 Originator Controlled Access Control | 91 |
| 7.4 Role-Based Access Control | 92 |
| 7.5 Summary | 94 |
| 7.6 Further Reading | 95 |
| 7.7 Exercises | 95 |
| Chapter 8 Basic Cryptography. | 97 |
| 8.1 What Is Cryptography? | 97 |
| 8.2 Classical Cryptosystems | 98 |
| 8.2.1 Transposition Ciphers | 99 |
| 8.2.2 Substitution Ciphers | 100 |
| 8.2.2.1 <i>Vigenere Cipher</i> | 101 |
| 8.2.2.2 <i>One-Time Pad</i> | 107 |
| 8.2.3 Data Encryption Standard | 108 |
| 8.2.4 Other Classical Ciphers | 112 |
| 8.3 Public Key Cryptography | 113 |
| 8.3.1 RSA | 114 |
| 8.4 Cryptographic Checksums | 116 |
| 8.4.1 HMAC | 118 |
| 8.5 Summary | 119 |
| 8.6 Further Reading | 119 |
| 8.7 Exercises | 120 |

| | |
|--|------------|
| Chapter 9 Key Management | 123 |
| 9.1 Session and Interchange Keys | 124 |
| 9.2 Key Exchange | 124 |
| 9.2.1 Classical Cryptographic Key Exchange and Authentication. | 125 |
| 9.2.2 Kerberos | 128 |
| 9.2.3 Public Key Cryptographic Key Exchange and Authentication | 129 |
| 9.3 Cryptographic Key Infrastructures | 130 |
| 9.3.1 Certificate Signature Chains | 131 |
| 9.3.1.1 X.509: Certification Signature Chains | 132 |
| 9.3.1.2 PGP Certificate Signature Chains | 134 |
| 9.3.2 Summary | 136 |
| 9.4 Storing and Revoking Keys | 136 |
| 9.4.1 Key Storage | 136 |
| 9.4.2 Key Revocation | 137 |
| 9.5 Digital Signatures | 137 |
| 9.5.1 Classical Signatures | 138 |
| 9.5.2 Public Key Signatures | 139 |
| 9.6 Summary | 140 |
| 9.7 Further Reading | 141 |
| 9.8 Exercises | 142 |
| | |
| Chapter 10 Cipher Techniques | 145 |
| 10.1 Problems | 145 |
| 10.1.1 Precomputing the Possible Messages | 145 |
| 10.1.2 Misordered Blocks | 146 |
| 10.1.3 Statistical Regularities | 146 |
| 10.1.4 Summary | 147 |
| 10.2 Stream and Block Ciphers | 147 |
| 10.2.1 Stream Ciphers | 148 |
| 10.2.1.1 Synchronous Stream Ciphers | 148 |
| 10.2.1.2 Self-Synchronous Stream Ciphers | 150 |
| 10.2.2 Block Ciphers | 151 |
| 10.2.2.1 Multiple Encryption | 152 |
| 10.3 Networks and Cryptography | 153 |
| 10.4 Example Protocols | 156 |
| 10.4.1 Secure Electronic Mail: PEM | 156 |
| 10.4.1.1 Design Principles | 157 |
| 10.4.1.2 Basic Design | 158 |
| 10.4.1.3 Other Considerations | 159 |
| 10.4.1.4 Conclusion | 160 |

| | | |
|-------------------|---|------------|
| 10.4.2 | Security at the Network Layer: IPsec | 161 |
| 10.4.2.1 | <i>IPsec Architecture</i> | 762 |
| 10.4.2.2 | <i>Authentication Header Protocol</i> | 765 |
| 10.4.2.3 | <i>Encapsulating Security Payload Protocol</i> | 766 |
| 10.4.3 | Conclusion | 167 |
| 10.5 | Summary | 168 |
| 10.6 | Further Reading | 168 |
| 10.7 | Exercises | 169 |
| Chapter 11 | Authentication | 171 |
| 11.1 | Authentication Basics | 171 |
| 11.2 | Passwords | 172 |
| 11.2.1 | Attacking a Password System | 174 |
| 11.2.2 | Countering Password Guessing | 175 |
| 11.2.2.1 | <i>Random Selection of Passwords</i> | 776 |
| 11.2.2.2 | <i>Pronounceable and Other Computer-Generated Passwords</i> | 777 |
| 11.2.2.3 | <i>User Selection of Passwords</i> | 178 |
| 11.2.2.4 | <i>Reusable Passwords and Dictionary Attacks</i> | 782 |
| 11.2.2.5 | <i>Guessing Through Authentication Functions</i> | 183 |
| 11.2.3 | ' Password Aging | 184 |
| 11.3 | Challenge-Response | 186 |
| 11.3.1 | Pass Algorithms | 186 |
| 11.3.2 | One-Time Passwords | 187 |
| 11.3.3 | Hardware-Supported Challenge-Response Procedures | 188 |
| 11.3.4 | Challenge-Response and Dictionary Attacks | 189 |
| 11.4 | Biometrics | 190 |
| 11.4.1 | Fingerprints | 190 |
| 11.4.2 | Voices | 191 |
| 11.4.3 | Eyes | 191 |
| 11.4.4 | Faces | 191 |
| 11.4.5 | Keystrokes | 192 |
| 11.4.6 | Combinations | 192 |
| 11.4.7 | Caution | 192 |
| 11.5 | Location | 193 |
| 11.6 | Multiple Methods | 193 |
| 11.7 | Summary | 195 |
| 11.8 | Further Reading | 196 |
| 11.9 | Exercises | 196 |

| | |
|--|------------|
| Chapter 12 Design Principles | 199 |
| 12.1 Overview | 199 |
| 12.2 Design Principles | 201 |
| 12.2.1 Principle of Least Privilege | 201 |
| 12.2.2 Principle of Fail-Safe Defaults | 202 |
| 12.2.3 Principle of Economy of Mechanism | 202 |
| 12.2.4 Principle of Complete Mediation | 203 |
| 12.2.5 Principle of Open Design | 204 |
| 12.2.6 Principle of Separation of Privilege | 205 |
| 12.2.7 Principle of Least Common Mechanism | 206 |
| 12.2.8 Principle of Psychological Acceptability | 206 |
| 12.3 Summary | 207 |
| 12.4 Further Reading | 208 |
| 12.5 Exercises | 208 |
| | |
| Chapter 13 Representing Identity | 211 |
| 13.1 What Is Identity? | 211 |
| 13.2 Files and Objects | 212 |
| 13.3 Users | 213 |
| 13.4 Groups and Roles | 214 |
| 13.5 Naming and Certificates | 215 |
| 13.5.1 The Meaning of the Identity | 218 |
| 13.5.2 Trust | 220 |
| 13.6 Identity on the Web | 221 |
| 13.6.1 Host Identity | 221 |
| 13.6.1.1 <i>Static and Dynamic Identifiers</i> | 222 |
| 13.6.1.2 <i>Security Issues with the Domain Name Service</i> | 224 |
| 13.6.2 State and Cookies | 225 |
| 13.6.3 Anonymity on the Web | 226 |
| 13.6.3.1 <i>Anonymity for Better or Worse</i> | 230 |
| 13.7 Summary | 233 |
| 13.8 Further Reading | 233 |
| 13.9 Exercises | 234 |
| | |
| Chapter 14 Access Control Mechanisms | 237 |
| 14.1 Access Control Lists | 237 |
| 14.1.1 Abbreviations of Access Control Lists | 238 |
| 14.1.2 Creation and Maintenance of Access Control Lists | 240 |
| 14.1.2.1 <i>Which Subjects Can Modify an Object's ACL?</i> | 241 |
| 14.1.2.2 <i>Do the ACLs Apply to a Privileged User?</i> | 241 |
| 14.1.2.3 <i>Does the ACL Support Groups and Wildcards?</i> | 242 |

| | | |
|-------------------|--|------------|
| 14.1.2.4 | <i>Conflicts</i> | 242 |
| 14.1.2.5 | <i>ACLs and Default Permissions</i> | 243 |
| 14.1.3 | Revocation of Rights | 243 |
| 14.1.4 | Example: Windows NT Access Control Lists | 244 |
| 14.2 | Capabilities | 246 |
| 14.2.1 | Implementation of Capabilities | 247 |
| 14.2.2 | Copying and Amplifying Capabilities | 248 |
| 14.2.3 | Revocation of Rights | 249 |
| 14.2.4 | Limits of Capabilities | 250 |
| 14.2.5 | Comparison with Access Control Lists | 251 |
| 14.3 | Locks and Keys | 252 |
| 14.3.1 | Type Checking | 253 |
| 14.4 | Ring-Based Access Control | 255 |
| 14.5 | Propagated Access Control Lists | 257 |
| 14.6 | Summary | 258 |
| 14.7 | Further Reading | 258 |
| 14.8 | Exercises | 259 |
| Chapter 15 | Information Flow | 261 |
| 15.1 | Basics and Background | 261 |
| 15.1.1 | Information Flow Models and Mechanisms | 263 |
| 15.2 | Compiler-Based Mechanisms | 263 |
| 15.2.1 | Declarations | 264 |
| 15.2.2 | Program Statements | 266 |
| 15.2.2.1 | <i>Assignment Statements</i> | 266 |
| 15.2.2.2 | <i>Compound Statements</i> | 267 |
| 15.2.2.3 | <i>Conditional Statements</i> | 267 |
| 15.2.2.4 | <i>Iterative Statements</i> | 268 |
| 15.2.2.5 | <i>Goto Statements</i> | 269 |
| 15.2.2.6 | <i>Procedure Calls</i> | 272 |
| 15.2.3 | Exceptions and Infinite Loops | 272 |
| 15.2.4 | Concurrency | 274 |
| 15.2.5 | Soundness | 276 |
| 15.3 | Execution-Based Mechanisms | 277 |
| 15.3.1 | Fenton's Data Mark Machine | 278 |
| 15.3.2 | Variable Classes | 280 |
| 15.4 | Example Information Flow Controls | 281 |
| 15.4.1 | Security Pipeline Interface | 282 |
| 15.4.2 | Secure Network Server Mail Guard | 282 |
| 15.5 | Summary | 284 |
| 15.6 | Further Reading | 284 |
| 15.7 | Exercises | 285 |

| | |
|--|------------|
| Chapter 16 Confinement Problem | 287 |
| 16.1 The Confinement Problem | 287 |
| 16.2 Isolation | 290 |
| 16.2.1 Virtual Machines | 290 |
| 16.2.2 Sandboxes | 292 |
| 16.3 Covert Channels | 294 |
| 16.3.1 Detection of Covert Channels | 296 |
| 16.3.2 Mitigation of Covert Channels | 303 |
| 16.4 Summary | 306 |
| 16.5 Further Reading | 306 |
| 16.6 Exercises | 307 |
| | |
| Chapter 17 Introduction to Assurance | 309 |
| 17.1 Assurance and Trust | 309 |
| 17.1.1 The Need for Assurance | 311 |
| 17.1.2 The Role of Requirements in Assurance | 313 |
| 17.1.3 Assurance Throughout the Life Cycle | 314 |
| 17.2 Building Secure and Trusted Systems | 316 |
| 17.2.1 Life Cycle | 316 |
| 17.2.1.1 <i>Conception</i> | 377 |
| 17.2.1.2 <i>Manufacture</i> | 318 |
| 17.2.1.3 <i>Deployment</i> | 319 |
| 17.2.1.4 <i>Fielded Product Life</i> | 320 |
| 17.2.2 The Waterfall Life Cycle Model | 320 |
| 17.2.2.1 <i>Requirements Definition and Analysis</i> | 320 |
| 17.2.2.2 <i>System and Software Design</i> | 327 |
| 17.2.2.3 <i>Implementation and Unit Testing</i> | 327 |
| 17.2.2.4 <i>Integration and System Testing</i> | 322 |
| 17.2.2.5 <i>Operation and Maintenance</i> | 322 |
| 17.2.2.6 <i>Discussion</i> | 322 |
| 17.2.3 Other Models of Software Development | 323 |
| 17.2.3.1 <i>Exploratory Programming</i> | 323 |
| 17.2.3.2 <i>Prototyping</i> | 323 |
| 17.2.3.3 <i>Formal Transformation</i> | 323 |
| 17.2.3.4 <i>System Assembly from Reusable Components</i> | 324 |
| 17.2.3.5 <i>Extreme Programming</i> | 324 |
| 17.3 Building Security In or Adding Security Later | 324 |
| 17.4 Summary | 328 |
| 17.5 Further Reading | 328 |
| 17.6 Exercises | 329 |

| | |
|--|------------|
| Chapter 18 Evaluating Systems | 331 |
| 18.1 Goals of Formal Evaluation | 331 |
| 18.1.1 Deciding to Evaluate. | 332 |
| 18.1.2 Historical Perspective of Evaluation Methodologies. | 333 |
| 18.2 TCSEC: 1983-1999. | 334 |
| 18.2.1 TCSEC Requirements. | 335 |
| 18.2.1.1 <i>TCSEC Functional Requirements</i> | 335 |
| 18.2.1.2 <i>TCSEC Assurance Requirements</i> | 336 |
| 18.2.2 The TCSEC Evaluation Classes. | 337 |
| 18.2.3 The TCSEC Evaluation Process. | 338 |
| 18.2.4 Impacts. | 338 |
| 18.2.4.1 <i>Scope Limitations</i> | 339 |
| 18.2.4.2 <i>Process Limitations</i> | 339 |
| 18.2.4.3 <i>Contributions</i> | 340 |
| 18.3 FIPS 140: 1994-Present | 341 |
| 18.3.1 FIPS 140 Requirements. | 341 |
| 18.3.2 FIPS 140-2 Security Levels. | 342 |
| 18.3.3 Impact | 342 |
| 18.4 The Common Criteria: 1998-Present | 343 |
| 18.4.1 Overview of the Methodology. | 344 |
| 18.4.2 CC Requirements. | 348 |
| 18.4.3 CC Security Functional Requirements. | 349 |
| 18.4.4 Assurance Requirements. | 351 |
| 18.4.5 Evaluation Assurance Levels. | 351 |
| 18.4.6 Evaluation Process. | 353 |
| 18.4.7 Impacts. | 354 |
| 18.4.8 Future of the Common Criteria | 354 |
| 18.4.8.1 <i>Interpretations</i> | 355 |
| 18.4.8.2 <i>Assurance Class AMA and Family ALC_FLR</i> | 355 |
| 18.4.8.3 <i>Products Versus Systems</i> | 355 |
| 18.4.8.4 <i>Protection Profiles and Security Targets</i> | 355 |
| 18.4.8.5 <i>Assurance Class AVA</i> | 356 |
| 18.4.8.6 <i>EAL5</i> | 356 |
| 18.5 SSE-CMM: 1997-Present | 356 |
| 18.5.1 The SSE-CMM Model. | 357 |
| 18.5.2 Using the SSE-CMM. | 358 |
| 18.6 Summary. | 359 |
| 18.7 Further Reading. | 360 |
| 18.8 Exercises. | 361 |

| | |
|--|----------------|
| Chapter 19 Malicious Logic | 363 |
| 19.1 Introduction | 363 |
| 19.2 Trojan Horses | 364 |
| 19.3 Computer Viruses | 365 |
| 19.3.1 Boot Sector Infectors | 367 |
| 19.3.2 Executable Infectors | 368 |
| 19.3.3 Multipartite Viruses | 369 |
| 19.3.4 TSR Viruses | 370 |
| 19.3.5 Stealth Viruses | 370 |
| 19.3.6 Encrypted Viruses | 370 |
| 19.3.7 Polymorphic Viruses | 371 |
| 19.3.8 Macro Viruses | 372 |
| 19.4 Computer Worms | 373 |
| 19.5 Other Forms of Malicious Logic | 374 |
| 19.5.1 Rabbits and Bacteria | 374 |
| 19.5.2 Logic Bombs | 375 |
| 19.6 Defenses | 376 |
| 19.6.1 Malicious Logic Acting as Both Data and Instructions | 376 |
| 19.6.2 Malicious Logic Assuming the Identity of a User | 377 |
| 19.6.2.1 <i>Information Flow Metrics</i> | 377 |
| 19.6.2.2 <i>Reducing the Rights</i> | 378 |
| 19.6.2.3 <i>Sandboxing</i> | 357 |
| 19.6.3 Malicious Logic Crossing Protection Domain Boundaries by Sharing | 381 |
| 19.6.4 Malicious Logic Altering Files | 382 |
| 19.6.5 Malicious Logic Performing Actions Beyond Specification | 383 |
| 19.6.5.7 <i>Proof-Carrying Code</i> | 384 |
| 19.6.6 Malicious Logic Altering Statistical Characteristics | 384 |
| 19.6.7 The Notion of Trust | 385 |
| 19.7 Summary | 385 |
| 19.8 Further Reading | 386 |
| 19.9 Exercises | 386 |
| Chapter 20 Vulnerability Analysis | 389 |
| 20.1 Introduction | 389 |
| 20.2 Penetration Studies | 391 |
| 20.2.1 Goals | 391 |
| 20.2.2 Layering of Tests | 392 |
| 20.2.3 Methodology at Each Layer | 393 |
| 20.2.4 Flaw Hypothesis Methodology | 393 |

| | | |
|-------------------|--|------------|
| 20.2.4.1 | <i>Information Gathering and Flaw Hypothesis</i> | 394 |
| 20.2.4.2 | <i>Flaw Testing</i> | 395 |
| 20.2.4.3 | <i>Flaw Generalization</i> | 395 |
| 20.2.4.4 | <i>Flaw Elimination</i> | 396 |
| 20.2.5 | Example: Penetration of the Michigan Terminal System | 396 |
| 20.2.6 | Example: Compromise of a Burroughs System | 398 |
| 20.2.7 | Example: Penetration of a Corporate Computer System | 399 |
| 20.2.8 | Example: Penetrating a UNIX System | 400 |
| 20.2.9 | Example: Penetrating a Windows NT System | 402 |
| 20.2.10 | Debate | 403 |
| 20.2.11 | Conclusion | 404 |
| 20.3 | Vulnerability Classification | 404 |
| 20.3.1 | Two Security Flaws | 405 |
| 20.4 | Frameworks | 406 |
| 20.4.1 | The RISOS Study | 406 |
| 20.4.1.1 | <i>The Flaw Classes</i> | 408 |
| 20.4.1.2 | <i>Legacy</i> | 409 |
| 20.4.2 | Protection Analysis Model | 409 |
| 20.4.2.1 | <i>The Flaw Classes</i> | 410 |
| 20.4.2.2 | <i>Legacy</i> | 412 |
| 20.4.3 | The NRL Taxonomy | 412 |
| 20.4.3.1 | <i>The Flaw Classes</i> | 412 |
| 20.4.3.2 | <i>Legacy</i> | 414 |
| 20.4.4 | Aslam's Model | 414 |
| 20.4.4.1 | <i>The Flaw Classes</i> | 415 |
| 20.4.4.2 | <i>Legacy</i> | 415 |
| 20.4.5 | Comparison and Analysis | 415 |
| 20.4.5.1 | <i>The xterm Log File Flaw</i> | 416 |
| 20.4.5.2 | <i>The fingerd Buffer Overflow Flaw</i> | 418 |
| 20.5 | Summary | 419 |
| 20.6 | Further Reading | 420 |
| 20.7 | Exercises | 421 |
| Chapter 21 | Auditing | 423 |
| 21.1 | Definitions | 423 |
| 21.2 | Anatomy of an Auditing System | 424 |
| 21.2.1 | Logger | 424 |
| 21.2.2 | Analyzer | 426 |
| 21.2.3 | Notifier | 427 |
| 21.3 | Designing an Auditing System | 428 |
| 21.3.1 | Implementation Considerations | 429 |

| | | |
|-------------------|---|------------|
| 21.3.2 | Syntactic Issues | 429 |
| 21.3.3 | Log Sanitization | 431 |
| 21.3.4 | Application and System Logging | 433 |
| 21.4 | A Posteriori Design | 434 |
| 21.4.1 | Auditing to Detect Violations of a Known Policy | 435 |
| 21.4.1.1 | <i>State-Based Auditing</i> | 435 |
| 21.4.1.2 | <i>Transition-Based Auditing</i> | 436 |
| 21.4.2 | Auditing to Detect Known Violations of a Policy | 437 |
| 21.5 | Auditing Mechanisms | 438 |
| 21.5.1 | Secure Systems | 438 |
| 21.5.2 | Nonsecure Systems | 440 |
| 21.6 | Examples: Auditing File Systems | 441 |
| 21.6.1 | Audit Analysis of the NFS Version 2 Protocol | 441 |
| 21.6.2 | The Logging and Auditing File System (LAFS) | 445 |
| 21.6.3 | Comparison | 447 |
| 21.7 | Audit Browsing | 448 |
| 21.8 | Summary | 450 |
| 21.9 | Further Reading | 451 |
| 21.10 | Exercises | 451 |
| Chapter 22 | Intrusion Detection | 455 |
| 22.1 | Principles | 455 |
| 22.2 | Basic Intrusion Detection | 456 |
| 22.3 | Models | 458 |
| 22.3.1 | Anomaly Modeling | 459 |
| 22.3.2 | Misuse Modeling | 461 |
| 22.3.3 | Specification Modeling | 463 |
| 22.3.4 | Summary | 464 |
| 22.4 | Architecture | 465 |
| 22.4.1 | Agent | 465 |
| 22.4.1.1 | <i>Host-Based Information Gathering</i> | 466 |
| 22.4.1.2 | <i>Network-Based Information Gathering</i> | 467 |
| 22.4.1.3 | <i>Combining Sources</i> | 467 |
| 22.4.2 | Director | 469 |
| 22.4.3 | Notifier | 469 |
| 22.5 | Organization of Intrusion Detection Systems | 471 |
| 22.5.1 | Monitoring Network Traffic for Intrusions: NSM | 471 |
| 22.5.2 | Combining Host and Network Monitoring: DIDS | 472 |
| 22.5.3 | Autonomous Agents: AAFID | 475 |
| 22.6 | Intrusion Response | 476 |
| 22.6.1 | Incident Prevention | 476 |

| | | |
|-------------------|---|------------|
| 22.6.2 | Intrusion Handling | 477 |
| 22.6.2.1 | <i>Containment Phase</i> | 478 |
| 22.6.2.2 | <i>Eradication Phase</i> | 479 |
| 22.6.2.3 | <i>Follow-Up Phase</i> | 482 |
| 22.7 | Summary. | 484 |
| 22.8 | Further Reading | 484 |
| 22.9 | Exercises | 485 |
| Chapter 23 | Network Security. | 487 |
| 23.1 | Introduction | 487 |
| 23.2 | Policy Development | 488 |
| 23.2.1 | Data Classes. | 489 |
| 23.2.2 | User Classes. | 490 |
| 23.2.3 | Availability. | 492 |
| 23.2.4 | Consistency Check. | 492 |
| 23.3 | Network Organization. | 493 |
| 23.3.1 | Firewalls and Proxies. | 494 |
| 23.3.2 | Analysis of the Network Infrastructure. | 496 |
| 23.3.2.1 | <i>Outer Firewall Configuration</i> | 497 |
| 23.3.2.2 | <i>Inner Firewall Configuration</i> | 499 |
| 23.3.3 | In the DMZ. | 500 |
| 23.3.3.1 | <i>DMZ Mail Server</i> | 500 |
| 23.3.3.2 | <i>DMZ WWW Server</i> | 507 |
| 23.3.3.3 | <i>DMZ DNS Server</i> | 503 |
| 23.3.3.4 | <i>DMZ Log Server</i> | 503 |
| 23.3.3.5 | <i>Summary</i> | 504 |
| 23.3.4 | In the Internal Network. | 504 |
| 23.3.5 | General Comment on Assurance. | 506 |
| 23.4 | Availability and Network Flooding | 507 |
| 23.4.1 | Intermediate Hosts. | 507 |
| 23.4.2 | TCP State and Memory Allocations. | 508 |
| 23.5 | Anticipating Attacks. | 510 |
| 23.6 | Summary. | 512 |
| 23.7 | Further Reading | 512 |
| 23.8 | Exercises | 513 |
| Chapter 24 | System Security. | 517 |
| 24.1 | Introduction. | 517 |
| 24.2 | Policy. | 518 |
| 24.2.1 | The Web Server System in the DMZ. | 518 |
| 24.2.2 | The Development System. | 519 |

| | | |
|-------------------|---|------------|
| 24.2.3 | Comparison | 522 |
| 24.2.4 | Conclusion | 523 |
| 24.3 | Networks | 523 |
| 24.3.1 | The Web Server System in the DMZ | 524 |
| 24.3.2 | The Development System | 526 |
| 24.3.3 | Comparison | 528 |
| 24.4 | Users | 529 |
| 24.4.1 | The Web Server System in the DMZ | 529 |
| 24.4.2 | The Development System | 531 |
| 24.4.3 | Comparison | 534 |
| 24.5 | Authentication | 534 |
| 24.5.1 | The Web Server System in the DMZ | 535 |
| 24.5.2 | Development Network System | 535 |
| 24.5.3 | Comparison | 537 |
| 24.6 | Processes | 537 |
| 24.6.1 | The Web Server System in the DMZ | 537 |
| 24.6.2 | The Development System | 541 |
| 24.6.3 | Comparison | 542 |
| 24.7 | Files | 543 |
| 24.7.1 | The Web Server System in the DMZ | 543 |
| 24.7.2 | The Development System | 545 |
| 24.7.3 | Comparison | 547 |
| 24.8 | Retrospective | 549 |
| 24.8.1 | The Web Server System in the DMZ | 549 |
| 24.8.2 | The Development System | 550 |
| 24.9 | Summary | 550 |
| 24.10 | Further Reading | 551 |
| 24.11 | Exercises | 551 |
| Chapter 25 | User Security | 555 |
| 25.1 | Policy | 555 |
| 25.2 | Access | 556 |
| 25.2.1 | Passwords | 556 |
| 25.2.2 | The Login Procedure | 558 |
| 25.2.2.1 | <i>Trusted Hosts</i> | 560 |
| 25.2.3 | Leaving the System | 560 |
| 25.3 | Files and Devices | 562 |
| 25.3.1 | Files | 562 |
| 25.3.1.1 | <i>File Permissions on Creation</i> | 563 |
| 25.3.1.2 | <i>Group Access</i> | 564 |
| 25.3.1.3 | <i>File Deletion</i> | 565 |

| | | |
|-------------------|--|------------|
| 25.3.2 | Devices | 567 |
| 25.3.2.1 | <i>Writable Devices</i> | 567 |
| 25.3.2.2 | <i>Smart Terminals</i> | 567 |
| 25.3.2.3 | <i>Monitors and Window Systems</i> | 569 |
| 25.4 | Processes | 570 |
| 25.4.1 | Copying and Moving Files | 570 |
| 25.4.2 | Accidentally Overwriting Files | 571 |
| 25.4.3 | Encryption, Cryptographic Keys, and Passwords | 571 |
| 25.4.4 | Start-up Settings | 573 |
| 25.4.5 | Limiting Privileges | 573 |
| 25.4.6 | Malicious Logic | 574 |
| 25.5 | Electronic Communications | 575 |
| 25.5.1 | Automated Electronic Mail Processing | 575 |
| 25.5.2 | Failure to Check Certificates | 575 |
| 25.5.3 | Sending Unexpected Content | 576 |
| 25.6 | Summary | 576 |
| 25.7 | Further Reading | 577 |
| 25.8 | Exercises | 577 |
| Chapter 26 | Program Security | 579 |
| 26.1 | Introduction | 579 |
| 26.2 | Requirements and Policy | 580 |
| 26.2.1 | Requirements | 580 |
| 26.2.2 | Threats | 581 |
| 26.2.2.1 | <i>Group 1: Unauthorized Users Accessing Role Accounts</i> | 581 |
| 26.2.2.2 | <i>Group 2: Authorized Users Accessing Role Accounts</i> | 582 |
| 26.2.2.3 | <i>Summary</i> | 583 |
| 26.3 | Design | 583 |
| 26.3.1 | Framework | 584 |
| 26.3.1.1 | <i>User Interface</i> | 584 |
| 26.3.1.2 | <i>High-Level Design</i> | 584 |
| 26.3.2 | Access to Roles and Commands | 585 |
| 26.3.2.1 | <i>Interface</i> | 586 |
| 26.3.2.2 | <i>Internals</i> | 586 |
| 26.3.2.3 | <i>Storage of the Access Control Data</i> | 587 |
| 26A | Refinement and Implementation | 590 |
| 26.4.1 | First-Level Refinement | 590 |
| 26.4.2 | Second-Level Refinement | 591 |

| | | |
|----------|---|-----|
| 26.4.3 | Functions. | 594 |
| 26.4.3.1 | <i>Obtaining Location.</i> | 594 |
| 26.4.3.2 | <i>The Access Control Record.</i> | 595 |
| 26.4.3.3 | <i>Error Handling in the Reading and Matching Routines.</i> | 596 |
| 26.4.4 | Summary. | 597 |
| 26.5 | Common Security-Related Programming Problems. | 597 |
| 26.5.1 | Improper Choice of Initial Protection Domain. | 598 |
| 26.5.1.1 | <i>Process Privileges.</i> | 598 |
| 26.5.1.2 | <i>Access Control File Permissions.</i> | 600 |
| 26.5.1.3 | <i>Memory Protection.</i> | 607 |
| 26.5.1.4 | <i>Trust in the System.</i> | 602 |
| 26.5.2 | Improper Isolation of Implementation Detail. | 603 |
| 26.5.2.1 | <i>Resource Exhaustion and User Identifiers.</i> | 603 |
| 26.5.2.2 | <i>Validating the Access Control Entries.</i> | 604 |
| 26.5.2.3 | <i>Restricting the Protection Domain of the Role Process.</i> | 604 |
| 26.5.3 | Improper Change. | 605 |
| 26.5.3.1 | <i>Memory.</i> | 605 |
| 26.5.3.2 | <i>Changes in File Contents.</i> | 608 |
| 26.5.3.3 | <i>Race Conditions in File Accesses.</i> | 608 |
| 26.5.4 | Improper Naming. | 609 |
| 26.5.5 | Improper Deallocation or Deletion. | 611 |
| 26.5.6 | Improper Validation. | 612 |
| 26.5.6.1 | <i>Bounds Checking.</i> | 672 |
| 26.5.6.2 | <i>Type Checking.</i> | 673 |
| 26.5.6.3 | <i>Error Checking.</i> | 614 |
| 26.5.6.4 | <i>Checking for Valid, not Invalid, Data.</i> | 674 |
| 26.5.6.5 | <i>Checking Input.</i> | 675 |
| 26.5.6.6 | <i>Designing for Validation.</i> | 677 |
| 26.5.7 | Improper Indivisibility. | 617 |
| 26.5.8 | Improper Sequencing. | 618 |
| 26.5.9 | Improper Choice of Operand or Operation. | 619 |
| 26.5.10 | Summary. | 621 |
| 26.6 | Testing, Maintenance, and Operation. | 623 |
| 26.6.1 | Testing. | 624 |
| 26.6.1.1 | <i>Testing the Module.</i> | 625 |
| 26.6.2 | Testing Composed Modules. | 626 |
| 26.6.3 | Testing the Program. | 627 |
| 26.7 | Distribution. | 627 |
| 26.8 | Conclusion. | 629 |

| | |
|--|------------|
| 26.9 Summary | 629 |
| 26.10 Further Reading | 629 |
| 26.11 Exercises | 630 |
| Chapter 27 Lattices | 633 |
| 27.1 Basics | 633 |
| 27.2 Lattices | 635 |
| 27.3 Exercises | 635 |
| Chapter 28 The Extended Euclidean Algorithm | 637 |
| 28.1 The Euclidean Algorithm | 637 |
| 28.2 The Extended Euclidean Algorithm | 638 |
| 28.3 Solving $ax \bmod n = 1$ | 640 |
| 28.4 Solving $ax \bmod n = b$ | 640 |
| 28.5 Exercises | 641 |
| Chapter 29 Virtual Machines | 643 |
| 29.1 Virtual Machine Structure | 643 |
| 29.2 Virtual Machine Monitor | 644 |
| 29.2.1 Privilege and Virtual Machines | 645 |
| 29.2.2 Physical Resources and Virtual Machines | 646 |
| 29.2.3 Paging and Virtual Machines | 647 |
| 29.3 Exercises | 648 |
| Bibliography | 649 |
| Index | 713 |