



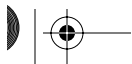
# Contents

---

<b>Preface</b> .....	<b>xxix</b>
Goals .....	xxx
Philosophy .....	xxxix
Organization .....	xxxiii
Roadmap .....	xxxiv
Dependencies .....	xxxiv
Background .....	xxxv
Undergraduate Level .....	xxxvi
Graduate Level .....	xxxvi
Practitioners .....	xxxviii
Special Acknowledgment .....	xxxviii
Acknowledgments .....	xxxviii

## **PART 1: INTRODUCTION** **1**

<b>Chapter 1 An Overview of Computer Security</b> .....	<b>3</b>
1.1 The Basic Components .....	3
1.1.1 Confidentiality .....	4
1.1.2 Integrity .....	5
1.1.3 Availability .....	6
1.2 Threats .....	6
1.3 Policy and Mechanism .....	9
1.3.1 Goals of Security .....	10
1.4 Assumptions and Trust .....	11
1.5 Assurance .....	12
1.5.1 Specification .....	13
1.5.2 Design .....	14
1.5.3 Implementation .....	14
1.6 Operational Issues .....	16
1.6.1 Cost-Benefit Analysis .....	16
1.6.2 Risk Analysis .....	17
1.6.3 Laws and Customs .....	18





vi Contents

1.7 Human Issues ..... 19  
    1.7.1 Organizational Problems ..... 20  
    1.7.2 People Problems ..... 21  
1.8 Tying It All Together ..... 22  
1.9 Summary ..... 23  
1.10 Research Issues ..... 24  
1.11 Further Readings ..... 24  
1.12 Exercises ..... 25

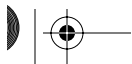
**PART 2: FOUNDATIONS 29**

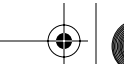
**Chapter 2 Access Control Matrix ..... 31**

2.1 Protection State ..... 31  
2.2 Access Control Matrix Model ..... 32  
    2.2.1 Access Control by Boolean Expression Evaluation ..... 35  
    2.2.2 Access Controlled by History ..... 36  
2.3 Protection State Transitions ..... 37  
    2.3.1 Conditional Commands ..... 40  
2.4 Copying, Owning, and the Attenuation of Privilege ..... 41  
    2.4.1 Copy Right ..... 42  
    2.4.2 Own Right ..... 42  
    2.4.3 Principle of Attenuation of Privilege ..... 43  
2.5 Summary ..... 43  
2.6 Research Issues ..... 44  
2.7 Further Reading ..... 44  
2.8 Exercises ..... 44

**Chapter 3 Foundational Results ..... 47**

3.1 The General Question ..... 47  
3.2 Basic Results ..... 48  
3.3 The Take-Grant Protection Model ..... 53  
    3.3.1 Sharing of Rights ..... 55  
    3.3.2 Interpretation of the Model ..... 58  
    3.3.3 Theft in the Take-Grant Protection Model ..... 60  
    3.3.4 Conspiracy ..... 63  
    3.3.5 Summary ..... 65  
3.4 Closing the Gap ..... 65  
    3.4.1 Schematic Protection Model ..... 66  
        3.4.1.1 *Link Predicate* ..... 66  
        3.4.1.2 *Filter Function* ..... 68





- 3.4.1.3 *Putting It All Together* .....68
- 3.4.1.4 *Demand and Create Operations*.....69
- 3.4.1.5 *Safety Analysis* .....72
- 3.5 Expressive Power and the Models .....78
  - 3.5.1 Brief Comparison of HRU and SPM.....78
  - 3.5.2 Extending SPM.....79
  - 3.5.3 Simulation and Expressiveness.....83
  - 3.5.4 Typed Access Matrix Model.....88
- 3.6 Summary .....90
- 3.7 Research Issues .....90
- 3.8 Further Reading .....91
- 3.9 Exercises .....91

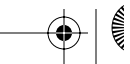
**PART 3: POLICY 93**

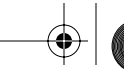
**Chapter 4 Security Policies ..... 95**

- 4.1 Security Policies .....95
- 4.2 Types of Security Policies .....99
- 4.3 The Role of Trust .....101
- 4.4 Types of Access Control .....103
- 4.5 Policy Languages .....104
  - 4.5.1 High-Level Policy Languages.....104
  - 4.5.2 Low-Level Policy Languages .....109
- 4.6 Example: Academic Computer Security Policy .....111
  - 4.6.1 General University Policy.....111
  - 4.6.2 Electronic Mail Policy.....112
    - 4.6.2.1 *The Electronic Mail Policy Summary* .....112
    - 4.6.2.2 *The Full Policy*.....113
    - 4.6.2.3 *Implementation at UC Davis* .....114
- 4.7 Security and Precision .....114
- 4.8 Summary .....119
- 4.9 Research Issues .....119
- 4.10 Further Reading .....120
- 4.11 Exercises .....120

**Chapter 5 Confidentiality Policies ..... 123**

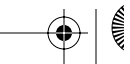
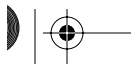
- 5.1 Goals of Confidentiality Policies .....123
- 5.2 The Bell-LaPadula Model .....124
  - 5.2.1 Informal Description.....124
  - 5.2.2 Example: The Data General B2 UNIX System.....128

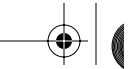




viii Contents

- 5.2.2.1 *Assigning MAC Labels* ..... 128
- 5.2.2.2 *Using MAC Labels* ..... 131
- 5.2.3 Formal Model ..... 132
  - 5.2.3.1 *Basic Security Theorem* ..... 134
  - 5.2.3.2 *Rules of Transformation* ..... 136
- 5.2.4 Example Model Instantiation: Multics ..... 139
  - 5.2.4.1 *The get-read Rule* ..... 140
  - 5.2.4.2 *The give-read Rule* ..... 141
- 5.3 Tranquility ..... 142
- 5.4 The Controversy over the Bell-LaPadula Model ..... 143
  - 5.4.1 McLean's  $\dagger$ -Property and the Basic Security Theorem ..... 143
  - 5.4.2 McLean's System Z and More Questions ..... 146
  - 5.4.3 Summary ..... 148
- 5.5 Summary ..... 148
- 5.6 Research Issues ..... 148
- 5.7 Further Reading ..... 149
- 5.8 Exercises ..... 150
  
- Chapter 6 Integrity Policies ..... 151**
  - 6.1 Goals ..... 151
  - 6.2 Biba Integrity Model ..... 153
    - 6.2.1 Low-Water-Mark Policy ..... 154
    - 6.2.2 Ring Policy ..... 155
    - 6.2.3 Biba's Model (Strict Integrity Policy) ..... 155
  - 6.3 Lipner's Integrity Matrix Model ..... 156
    - 6.3.1 Lipner's Use of the Bell-LaPadula Model ..... 156
    - 6.3.2 Lipner's Full Model ..... 158
    - 6.3.3 Comparison with Biba ..... 160
  - 6.4 Clark-Wilson Integrity Model ..... 160
    - 6.4.1 The Model ..... 161
      - 6.4.1.1 *A UNIX Approximation to Clark-Wilson* ..... 164
    - 6.4.2 Comparison with the Requirements ..... 164
    - 6.4.3 Comparison with Other Models ..... 165
  - 6.5 Summary ..... 166
  - 6.6 Research Issues ..... 166
  - 6.7 Further Reading ..... 167
  - 6.8 Exercises ..... 167
  
- Chapter 7 Hybrid Policies ..... 169**
  - 7.1 Chinese Wall Model ..... 169
    - 7.1.1 Informal Description ..... 170
    - 7.1.2 Formal Model ..... 172

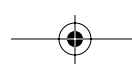
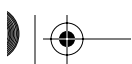




- 7.1.3 Bell-LaPadula and Chinese Wall Models . . . . . 175
- 7.1.4 Clark-Wilson and Chinese Wall Models . . . . . 177
- 7.2 Clinical Information Systems Security Policy . . . . . 177
  - 7.2.1 Bell-LaPadula and Clark-Wilson Models . . . . . 179
- 7.3 Originator Controlled Access Control . . . . . 180
- 7.4 Role-Based Access Control . . . . . 182
- 7.5 Summary . . . . . 184
- 7.6 Research Issues . . . . . 184
- 7.7 Further Reading . . . . . 184
- 7.8 Exercises . . . . . 185
  
- Chapter 8 Noninterference and Policy Composition . . . . . 187**
  - 8.1 The Problem . . . . . 187
    - 8.1.1 Composition of Bell-LaPadula Models . . . . . 188
  - 8.2 Deterministic Noninterference . . . . . 191
    - 8.2.1 Unwinding Theorem . . . . . 195
    - 8.2.2 Access Control Matrix Interpretation . . . . . 197
    - 8.2.3 Security Policies That Change over Time . . . . . 200
    - 8.2.4 Composition of Deterministic Noninterference-Secure Systems . . . 201
  - 8.3 Nondeducibility . . . . . 202
    - 8.3.1 Composition of Deducibly Secure Systems . . . . . 204
  - 8.4 Generalized Noninterference . . . . . 205
    - 8.4.1 Composition of Generalized Noninterference Systems . . . . . 206
  - 8.5 Restrictiveness . . . . . 208
    - 8.5.1 State Machine Model . . . . . 208
    - 8.5.2 Composition of Restrictive Systems . . . . . 209
  - 8.6 Summary . . . . . 210
  - 8.7 Research Issues . . . . . 211
  - 8.8 Further Reading . . . . . 211
  - 8.9 Exercises . . . . . 212

**PART 4: IMPLEMENTATION I: CRYPTOGRAPHY 215**

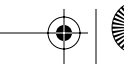
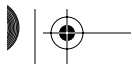
- Chapter 9 Basic Cryptography . . . . . 217**
  - 9.1 What Is Cryptography? . . . . . 217
  - 9.2 Classical Cryptosystems . . . . . 218
    - 9.2.1 Transposition Ciphers . . . . . 219
    - 9.2.2 Substitution Ciphers . . . . . 220
      - 9.2.2.1 *Vigenère Cipher* . . . . . 221
      - 9.2.2.2 *One-Time Pad* . . . . . 227





x Contents

- 9.2.3 Data Encryption Standard . . . . . 228
- 9.2.4 Other Classical Ciphers . . . . . 232
- 9.3 Public Key Cryptography . . . . . 233
  - 9.3.1 Diffie-Hellman . . . . . 233
  - 9.3.2 RSA . . . . . 234
- 9.4 Cryptographic Checksums . . . . . 237
  - 9.4.1 HMAC . . . . . 239
- 9.5 Summary . . . . . 239
- 9.6 Research Issues . . . . . 240
- 9.7 Further Reading . . . . . 240
- 9.8 Exercises . . . . . 241
  
- Chapter 10 Key Management . . . . . 245**
- 10.1 Session and Interchange Keys . . . . . 246
- 10.2 Key Exchange . . . . . 246
  - 10.2.1 Classical Cryptographic Key Exchange and Authentication. . . . . 247
  - 10.2.2 Kerberos . . . . . 250
  - 10.2.3 Public Key Cryptographic Key Exchange and Authentication . . . . . 251
- 10.3 Key Generation . . . . . 252
- 10.4 Cryptographic Key Infrastructures . . . . . 254
  - 10.4.1 Merkle's Tree Authentication Scheme . . . . . 255
  - 10.4.2 Certificate Signature Chains . . . . . 256
    - 10.4.2.1 X.509: Certification Signature Chains . . . . . 256
    - 10.4.2.2 PGP Certificate Signature Chains . . . . . 258
  - 10.4.3 Summary . . . . . 260
- 10.5 Storing and Revoking Keys . . . . . 261
  - 10.5.1 Key Storage . . . . . 261
    - 10.5.1.1 Key Escrow . . . . . 262
    - 10.5.1.2 Key Escrow System and the Clipper Chip . . . . . 263
    - 10.5.1.3 The Yaksha Security System . . . . . 264
    - 10.5.1.4 Other Approaches . . . . . 265
  - 10.5.2 Key Revocation . . . . . 265
- 10.6 Digital Signatures . . . . . 266
  - 10.6.1 Classical Signatures . . . . . 267
  - 10.6.2 Public Key Signatures . . . . . 267
    - 10.6.2.1 RSA Digital Signatures . . . . . 267
    - 10.6.2.2 El Gamal Digital Signature . . . . . 269
- 10.7 Summary . . . . . 270
- 10.8 Research Issues . . . . . 271
- 10.9 Further Reading . . . . . 272
- 10.10 Exercises . . . . . 272





- Chapter 11 Cipher Techniques ..... 275**
- 11.1 Problems ..... 275
  - 11.1.1 Precomputing the Possible Messages ..... 275
  - 11.1.2 Misordered Blocks ..... 276
  - 11.1.3 Statistical Regularities ..... 276
  - 11.1.4 Summary ..... 277
- 11.2 Stream and Block Ciphers ..... 277
  - 11.2.1 Stream Ciphers ..... 277
    - 11.2.1.1 Synchronous Stream Ciphers* ..... 278
    - 11.2.1.2 Self-Synchronous Stream Ciphers* ..... 280
  - 11.2.2 Block Ciphers ..... 281
    - 11.2.2.1 Multiple Encryption* ..... 282
- 11.3 Networks and Cryptography ..... 283
- 11.4 Example Protocols ..... 286
  - 11.4.1 Secure Electronic Mail: PEM ..... 286
    - 11.4.1.1 Design Principles* ..... 287
    - 11.4.1.2 Basic Design* ..... 288
    - 11.4.1.3 Other Considerations* ..... 289
    - 11.4.1.4 Conclusion* ..... 290
  - 11.4.2 Security at the Transport Layer: SSL ..... 291
    - 11.4.2.1 Supporting Cryptographic Mechanisms* ..... 292
    - 11.4.2.2 Lower Layer: SSL Record Protocol* ..... 294
    - 11.4.2.3 Upper Layer: SSL Handshake Protocol* ..... 295
    - 11.4.2.4 Upper Layer: SSL Change Cipher Spec Protocol* ..... 297
    - 11.4.2.5 Upper Layer: SSL Alert Protocol* ..... 297
    - 11.4.2.6 Upper Layer: Application Data Protocol* ..... 298
    - 11.4.2.7 Summary* ..... 298
  - 11.4.3 Security at the Network Layer: IPsec ..... 298
    - 11.4.3.1 IPsec Architecture* ..... 299
    - 11.4.3.2 Authentication Header Protocol* ..... 303
    - 11.4.3.3 Encapsulating Security Payload Protocol* ..... 304
  - 11.4.4 Conclusion ..... 305
- 11.5 Summary ..... 306
- 11.6 Research Issues ..... 306
- 11.7 Further Reading ..... 306
- 11.8 Exercises ..... 307
  
- Chapter 12 Authentication ..... 309**
- 12.1 Authentication Basics ..... 309
- 12.2 Passwords ..... 310
  - 12.2.1 Attacking a Password System ..... 312



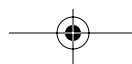


xii Contents

- 12.2.2 Countering Password Guessing . . . . . 313
  - 12.2.2.1 *Random Selection of Passwords* . . . . . 314
  - 12.2.2.2 *Pronounceable and Other Computer-Generated Passwords* . . . . . 315
  - 12.2.2.3 *User Selection of Passwords* . . . . . 316
  - 12.2.2.4 *Reusable Passwords and Dictionary Attacks* . . . . . 320
  - 12.2.2.5 *Guessing Through Authentication Functions* . . . . . 321
- 12.2.3 Password Aging . . . . . 322
- 12.3 Challenge-Response . . . . . 324
  - 12.3.1 Pass Algorithms . . . . . 324
  - 12.3.2 One-Time Passwords . . . . . 325
  - 12.3.3 Hardware-Supported Challenge-Response Procedures . . . . . 326
  - 12.3.4 Challenge-Response and Dictionary Attacks . . . . . 327
- 12.4 Biometrics . . . . . 328
  - 12.4.1 Fingerprints . . . . . 328
  - 12.4.2 Voices . . . . . 329
  - 12.4.3 Eyes . . . . . 329
  - 12.4.4 Faces . . . . . 329
  - 12.4.5 Keystrokes . . . . . 330
  - 12.4.6 Combinations . . . . . 330
  - 12.4.7 Caution . . . . . 330
- 12.5 Location . . . . . 331
- 12.6 Multiple Methods . . . . . 331
- 12.7 Summary . . . . . 333
- 12.8 Research Issues . . . . . 334
- 12.9 Further Reading . . . . . 335
- 12.10 Exercises . . . . . 335

**PART 5: IMPLEMENTATION II: SYSTEMS 339**

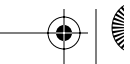
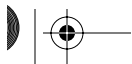
- Chapter 13 Design Principles . . . . . 341**
  - 13.1 Overview . . . . . 341
  - 13.2 Design Principles . . . . . 343
    - 13.2.1 Principle of Least Privilege . . . . . 343
    - 13.2.2 Principle of Fail-Safe Defaults . . . . . 344
    - 13.2.3 Principle of Economy of Mechanism . . . . . 344
    - 13.2.4 Principle of Complete Mediation . . . . . 345
    - 13.2.5 Principle of Open Design . . . . . 346
    - 13.2.6 Principle of Separation of Privilege . . . . . 347
    - 13.2.7 Principle of Least Common Mechanism . . . . . 348
    - 13.2.8 Principle of Psychological Acceptability . . . . . 348







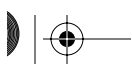
- 13.3 Summary ..... 349
- 13.4 Research Issues ..... 350
- 13.5 Further Reading ..... 350
- 13.6 Exercises ..... 351
  
- Chapter 14 Representing Identity ..... 353**
- 14.1 What Is Identity? ..... 353
- 14.2 Files and Objects ..... 354
- 14.3 Users ..... 355
- 14.4 Groups and Roles ..... 356
- 14.5 Naming and Certificates ..... 357
  - 14.5.1 Conflicts ..... 360
  - 14.5.2 The Meaning of the Identity ..... 363
  - 14.5.3 Trust ..... 364
- 14.6 Identity on the Web ..... 366
  - 14.6.1 Host Identity ..... 366
    - 14.6.1.1 *Static and Dynamic Identifiers* ..... 367
    - 14.6.1.2 *Security Issues with the Domain Name Service* ..... 368
  - 14.6.2 State and Cookies ..... 369
  - 14.6.3 Anonymity on the Web ..... 371
    - 14.6.3.1 *Anonymity for Better or Worse* ..... 375
- 14.7 Summary ..... 377
- 14.8 Research Issues ..... 378
- 14.9 Further Reading ..... 378
- 14.10 Exercises ..... 379
  
- Chapter 15 Access Control Mechanisms ..... 381**
- 15.1 Access Control Lists ..... 381
  - 15.1.1 Abbreviations of Access Control Lists ..... 382
  - 15.1.2 Creation and Maintenance of Access Control Lists ..... 384
    - 15.1.2.1 *Which Subjects Can Modify an Object's ACL?* ..... 385
    - 15.1.2.2 *Do the ACLs Apply to a Privileged User?* ..... 385
    - 15.1.2.3 *Does the ACL Support Groups and Wildcards?* ..... 386
    - 15.1.2.4 *Conflicts* ..... 386
    - 15.1.2.5 *ACLs and Default Permissions* ..... 387
  - 15.1.3 Revocation of Rights ..... 387
  - 15.1.4 Example: Windows NT Access Control Lists ..... 388
- 15.2 Capabilities ..... 390
  - 15.2.1 Implementation of Capabilities ..... 391
  - 15.2.2 Copying and Amplifying Capabilities ..... 392
  - 15.2.3 Revocation of Rights ..... 393
  - 15.2.4 Limits of Capabilities ..... 394

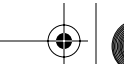




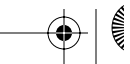
xiv Contents

- 15.2.5 Comparison with Access Control Lists . . . . . 395
- 15.3 Locks and Keys . . . . . 396
  - 15.3.1 Type Checking . . . . . 397
  - 15.3.2 Sharing Secrets . . . . . 399
- 15.4 Ring-Based Access Control . . . . . 400
- 15.5 Propagated Access Control Lists . . . . . 402
- 15.6 Summary . . . . . 404
- 15.7 Research Issues . . . . . 404
- 15.8 Further Reading . . . . . 405
- 15.9 Exercises . . . . . 405
  
- Chapter 16 Information Flow . . . . . 407**
- 16.1 Basics and Background . . . . . 407
  - 16.1.1 Entropy-Based Analysis . . . . . 408
  - 16.1.2 Information Flow Models and Mechanisms . . . . . 409
- 16.2 Nonlattice Information Flow Policies . . . . . 410
  - 16.2.1 Confinement Flow Model . . . . . 411
  - 16.2.2 Transitive Nonlattice Information Flow Policies . . . . . 412
  - 16.2.3 Nontransitive Information Flow Policies . . . . . 413
- 16.3 Compiler-Based Mechanisms . . . . . 415
  - 16.3.1 Declarations . . . . . 416
  - 16.3.2 Program Statements . . . . . 418
    - 16.3.2.1 *Assignment Statements* . . . . . 418
    - 16.3.2.2 *Compound Statements* . . . . . 419
    - 16.3.2.3 *Conditional Statements* . . . . . 419
    - 16.3.2.4 *Iterative Statements* . . . . . 420
    - 16.3.2.5 *Goto Statements* . . . . . 421
    - 16.3.2.6 *Procedure Calls* . . . . . 424
  - 16.3.3 Exceptions and Infinite Loops . . . . . 424
  - 16.3.4 Concurrency . . . . . 426
  - 16.3.5 Soundness . . . . . 428
- 16.4 Execution-Based Mechanisms . . . . . 429
  - 16.4.1 Fenton's Data Mark Machine . . . . . 430
  - 16.4.2 Variable Classes . . . . . 432
- 16.5 Example Information Flow Controls . . . . . 433
  - 16.5.1 Security Pipeline Interface . . . . . 434
  - 16.5.2 Secure Network Server Mail Guard . . . . . 434
- 16.6 Summary . . . . . 436
- 16.7 Research Issues . . . . . 436
- 16.8 Further Reading . . . . . 437
- 16.9 Exercises . . . . . 437





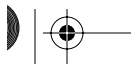
<b>Chapter 17 Confinement Problem</b> .....	<b>439</b>
17.1 The Confinement Problem .....	439
17.2 Isolation .....	442
17.2.1 Virtual Machines .....	442
17.2.2 Sandboxes .....	444
17.3 Covert Channels .....	446
17.3.1 Detection of Covert Channels .....	448
17.3.1.1 <i>Noninterference</i> .....	448
17.3.1.2 <i>The Shared Resource Matrix Methodology</i> .....	450
17.3.1.3 <i>Information Flow Analysis</i> .....	453
17.3.1.4 <i>Covert Flow Trees</i> .....	454
17.3.2 Analysis of Covert Channels .....	462
17.3.2.1 <i>Covert Channel Capacity and Noninterference</i> .....	462
17.3.2.2 <i>Measuring Covert Channel Capacity</i> .....	464
17.3.2.3 <i>Analyzing a Noisy Covert Channel's Capacity</i> .....	465
17.3.3 Mitigation of Covert Channels .....	467
17.4 Summary .....	470
17.5 Research Issues .....	471
17.6 Further Reading .....	472
17.7 Exercises .....	472
<b>PART 6: ASSURANCE</b> .....	<b>475</b>
<b>Chapter 18 Introduction to Assurance</b> .....	<b>477</b>
18.1 Assurance and Trust .....	477
18.1.1 The Need for Assurance .....	479
18.1.2 The Role of Requirements in Assurance .....	481
18.1.3 Assurance Throughout the Life Cycle .....	482
18.2 Building Secure and Trusted Systems .....	484
18.2.1 Life Cycle .....	484
18.2.1.1 <i>Conception</i> .....	485
18.2.1.2 <i>Manufacture</i> .....	486
18.2.1.3 <i>Deployment</i> .....	487
18.2.1.4 <i>Fielded Product Life</i> .....	488
18.2.2 The Waterfall Life Cycle Model .....	488
18.2.2.1 <i>Requirements Definition and Analysis</i> .....	488
18.2.2.2 <i>System and Software Design</i> .....	489
18.2.2.3 <i>Implementation and Unit Testing</i> .....	489
18.2.2.4 <i>Integration and System Testing</i> .....	490
18.2.2.5 <i>Operation and Maintenance</i> .....	490
18.2.2.6 <i>Discussion</i> .....	490





xvi Contents

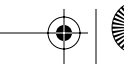
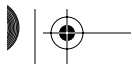
- 18.2.3 Other Models of Software Development. . . . . 491
  - 18.2.3.1 *Exploratory Programming* . . . . . 491
  - 18.2.3.2 *Prototyping* . . . . . 491
  - 18.2.3.3 *Formal Transformation* . . . . . 491
  - 18.2.3.4 *System Assembly from Reusable Components* . . . . . 492
  - 18.2.3.5 *Extreme Programming* . . . . . 492
- 18.3 Summary . . . . . 492
- 18.4 Research Issues . . . . . 493
- 18.5 Further Reading . . . . . 494
- 18.6 Exercises . . . . . 494
  
- Chapter 19 Building Systems with Assurance . . . . . 497**
- 19.1 Assurance in Requirements Definition and Analysis . . . . . 497
  - 19.1.1 Threats and Security Objectives . . . . . 498
  - 19.1.2 Architectural Considerations . . . . . 499
    - 19.1.2.1 *Security Mechanisms and Layered Architecture* . . . . . 500
    - 19.1.2.2 *Building Security in or Adding Security Later* . . . . . 501
  - 19.1.3 Policy Definition and Requirements Specification . . . . . 505
  - 19.1.4 Justifying Requirements . . . . . 508
- 19.2 Assurance During System and Software Design . . . . . 510
  - 19.2.1 Design Techniques That Support Assurance. . . . . 510
  - 19.2.2 Design Document Contents. . . . . 512
    - 19.2.2.1 *Security Functions Summary Specification* . . . . . 513
    - 19.2.2.2 *External Functional Specification* . . . . . 513
    - 19.2.2.3 *Internal Design Description* . . . . . 515
    - 19.2.2.4 *Internal Design Specification* . . . . . 520
  - 19.2.3 Building Documentation and Specifications . . . . . 521
    - 19.2.3.1 *Modification Specifications* . . . . . 521
    - 19.2.3.2 *Security Specifications* . . . . . 522
    - 19.2.3.3 *Formal Specifications* . . . . . 523
  - 19.2.4 Justifying That Design Meets Requirements. . . . . 523
    - 19.2.4.1 *Requirements Tracing and Informal Correspondence* . 523
    - 19.2.4.2 *Informal Arguments* . . . . . 526
    - 19.2.4.3 *Formal Methods: Proof Techniques* . . . . . 527
    - 19.2.4.4 *Review* . . . . . 528
      - Example: Setting up the Review* . . . . . 529
      - Example: The Technical Review* . . . . . 529
      - Example: The Review Meeting* . . . . . 530
      - Example: Completion of the Review* . . . . . 531
- 19.3 Assurance in Implementation and Integration . . . . . 531
  - 19.3.1 Implementation Considerations That Support Assurance . . . . . 531



- 19.3.2 Assurance Through Implementation Management . . . . . 532
- 19.3.3 Justifying That the Implementation Meets the Design. . . . . 533
  - 19.3.3.1 Security Testing . . . . . 533
  - 19.3.3.2 Security Testing Using PGWG . . . . . 536
  - 19.3.3.2 Test Matrices . . . . . 536
  - Example: Test Assertions . . . . . 538
  - Example: Test Specifications . . . . . 539
  - 19.3.3.3 Formal Methods: Proving That Programs Are Correct 541
- 19.4 Assurance During Operation and Maintenance . . . . . 541
- 19.5 Summary . . . . . 541
- 19.6 Research Issues . . . . . 542
- 19.7 Further Reading . . . . . 542
- 19.8 Exercises . . . . . 543
- Chapter 20 Formal Methods . . . . . 545**
- 20.1 Formal Verification Techniques . . . . . 545
- 20.2 Formal Specification . . . . . 548
- 20.3 Early Formal Verification Techniques . . . . . 551
  - 20.3.1 The Hierarchical Development Methodology . . . . . 551
    - 20.3.1.1 Verification in HDM . . . . . 553
    - 20.3.1.2 The Boyer-Moore Theorem Prover . . . . . 555
  - 20.3.2 Enhanced HDM . . . . . 556
  - 20.3.3 The Gypsy Verification Environment . . . . . 557
    - 20.3.3.1 The Gypsy Language . . . . . 557
    - 20.3.3.2 The Bledsoe Theorem Prover . . . . . 558
- 20.4 Current Verification Systems . . . . . 559
  - 20.4.1 The Prototype Verification System . . . . . 559
    - 20.4.1.1 The PVS Specification Language. . . . . 559
    - 20.4.1.2 The PVS Proof Checker . . . . . 561
    - 20.4.1.3 Experience with PVS . . . . . 562
  - 20.4.2 The Symbolic Model Verifier . . . . . 562
    - 20.4.2.1 The SMV Language . . . . . 562
    - 20.4.2.2 The SMV Proof Theory . . . . . 564
    - 20.4.2.3 SMV Experience. . . . . 566
  - 20.4.3 The Naval Research Laboratory Protocol Analyzer. . . . . 566
    - 20.4.3.1 NPA Languages . . . . . 566
    - 20.4.3.2 NPA Experience. . . . . 567
- 20.5 Summary . . . . . 567
- 20.6 Research Issues . . . . . 568
- 20.7 Further Reading . . . . . 568
- 20.8 Exercises . . . . . 569



<b>Chapter 21 Evaluating Systems</b> .....	<b>571</b>
21.1 Goals of Formal Evaluation .....	571
21.1.1 Deciding to Evaluate .....	572
21.1.2 Historical Perspective of Evaluation Methodologies .....	573
21.2 TCSEC: 1983–1999 .....	574
21.2.1 TCSEC Requirements .....	575
21.2.1.1 <i>TCSEC Functional Requirements</i> .....	575
21.2.1.2 <i>TCSEC Assurance Requirements</i> .....	576
21.2.2 The TCSEC Evaluation Classes .....	577
21.2.3 The TCSEC Evaluation Process .....	578
21.2.4 Impacts .....	578
21.2.4.1 <i>Scope Limitations</i> .....	579
21.2.4.2 <i>Process Limitations</i> .....	579
21.2.4.3 <i>Contributions</i> .....	580
21.3 International Efforts and the ITSEC: 1991–2001 .....	581
21.3.1 ITSEC Assurance Requirements .....	582
21.3.1.1 <i>Requirements in the TCSEC Not Found in the ITSEC</i> .	582
21.3.1.2 <i>Requirements in the ITSEC Not Found in the TCSEC</i> .	583
21.3.2 The ITSEC Evaluation Levels .....	583
21.3.3 The ITSEC Evaluation Process .....	584
21.3.4 Impacts .....	585
21.3.4.1 <i>Vendor Provided Security Targets</i> .....	585
21.3.4.2 <i>Process Limitations</i> .....	585
21.4 Commercial International Security Requirements: 1991 .....	586
21.4.1 CISR Requirements .....	586
21.4.2 Impacts .....	587
21.5 Other Commercial Efforts: Early 1990s .....	587
21.6 The Federal Criteria: 1992 .....	587
21.6.1 FC Requirements .....	588
21.6.2 Impacts .....	588
21.7 FIPS 140: 1994–Present .....	589
21.7.1 FIPS 140 Requirements .....	589
21.7.2 FIPS 140-2 Security Levels .....	590
21.7.3 Impact .....	591
21.8 The Common Criteria: 1998–Present .....	591
21.8.1 Overview of the Methodology .....	592
21.8.2 CC Requirements .....	596
21.8.3 CC Security Functional Requirements .....	597
21.8.4 Assurance Requirements .....	599
21.8.5 Evaluation Assurance Levels .....	599
21.8.6 Evaluation Process .....	601



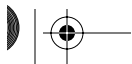


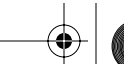
- 21.8.7 Impacts . . . . . 602
- 21.8.8 Future of the Common Criteria . . . . . 602
  - 21.8.8.1 Interpretations . . . . . 602
  - 21.8.8.2 Assurance Class AMA and Family ALC\_FLR . . . . . 603
  - 21.8.8.3 Products Versus Systems . . . . . 603
  - 21.8.8.4 Protection Profiles and Security Targets . . . . . 603
  - 21.8.8.5 Assurance Class AVA . . . . . 603
  - 21.8.8.6 EAL5 . . . . . 604
- 21.9 SSE-CMM: 1997–Present . . . . . 604
  - 21.9.1 The SSE-CMM Model . . . . . 604
  - 21.9.2 Using the SSE-CMM . . . . . 606
- 21.10 Summary . . . . . 607
- 21.11 Research Issues . . . . . 608
- 21.12 Further Reading . . . . . 608
- 21.13 Exercises . . . . . 609

**PART 7: SPECIAL TOPICS 611**

**Chapter 22 Malicious Logic . . . . . 613**

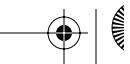
- 22.1 Introduction . . . . . 613
- 22.2 Trojan Horses . . . . . 614
- 22.3 Computer Viruses . . . . . 615
  - 22.3.1 Boot Sector Infectors . . . . . 617
  - 22.3.2 Executable Infectors . . . . . 618
  - 22.3.3 Multipartite Viruses . . . . . 619
  - 22.3.4 TSR Viruses . . . . . 620
  - 22.3.5 Stealth Viruses . . . . . 620
  - 22.3.6 Encrypted Viruses . . . . . 620
  - 22.3.7 Polymorphic Viruses . . . . . 621
  - 22.3.8 Macro Viruses . . . . . 622
- 22.4 Computer Worms . . . . . 623
- 22.5 Other Forms of Malicious Logic . . . . . 624
  - 22.5.1 Rabbits and Bacteria . . . . . 624
  - 22.5.2 Logic Bombs . . . . . 625
- 22.6 Theory of Malicious Logic . . . . . 626
  - 22.6.1 Theory of Computer Viruses . . . . . 626
- 22.7 Defenses . . . . . 630
  - 22.7.1 Malicious Logic Acting as Both Data and Instructions . . . . . 630
  - 22.7.2 Malicious Logic Assuming the Identity of a User . . . . . 631
    - 22.7.2.1 Information Flow Metrics . . . . . 631





xx Contents

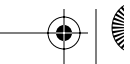
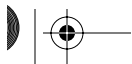
- 22.7.2.2 *Reducing the Rights* . . . . . 632
- 22.7.2.3 *Sandboxing* . . . . . 635
- 22.7.3 Malicious Logic Crossing Protection
  - Domain Boundaries by Sharing . . . . . 636
- 22.7.4 Malicious Logic Altering Files . . . . . 637
- 22.7.5 Malicious Logic Performing Actions Beyond Specification. . . . . 638
  - 22.7.5.1 *Proof-Carrying Code* . . . . . 638
- 22.7.6 Malicious Logic Altering Statistical Characteristics. . . . . 639
- 22.7.7 The Notion of Trust. . . . . 640
- 22.8 Summary . . . . . 640
- 22.9 Research Issues . . . . . 640
- 22.10 Further Reading . . . . . 641
- 22.11 Exercises . . . . . 642
  
- Chapter 23 Vulnerability Analysis . . . . . 645**
- 23.1 Introduction . . . . . 645
- 23.2 Penetration Studies . . . . . 647
  - 23.2.1 Goals . . . . . 647
  - 23.2.2 Layering of Tests . . . . . 648
  - 23.2.3 Methodology at Each Layer . . . . . 649
  - 23.2.4 Flaw Hypothesis Methodology . . . . . 649
    - 23.2.4.1 *Information Gathering and Flaw Hypothesis* . . . . . 650
    - 23.2.4.2 *Flaw Testing* . . . . . 651
    - 23.2.4.3 *Flaw Generalization* . . . . . 651
    - 23.2.4.4 *Flaw Elimination* . . . . . 652
  - 23.2.5 Example: Penetration of the Michigan Terminal System . . . . . 652
  - 23.2.6 Example: Compromise of a Burroughs System . . . . . 654
  - 23.2.7 Example: Penetration of a Corporate Computer System. . . . . 655
  - 23.2.8 Example: Penetrating a UNIX System . . . . . 656
  - 23.2.9 Example: Penetrating a Windows NT System . . . . . 658
  - 23.2.10 Debate . . . . . 659
  - 23.2.11 Conclusion. . . . . 660
- 23.3 Vulnerability Classification . . . . . 660
  - 23.3.1 Two Security Flaws. . . . . 661
- 23.4 Frameworks . . . . . 662
  - 23.4.1 The RISOS Study . . . . . 662
    - 23.4.1.1 *The Flaw Classes* . . . . . 664
    - 23.4.1.2 *Legacy*. . . . . 665
  - 23.4.2 Protection Analysis Model . . . . . 665
    - 23.4.2.1 *The Flaw Classes* . . . . . 666
    - 23.4.2.2 *Analysis Procedure* . . . . . 668
    - 23.4.2.3 *Legacy*. . . . . 670

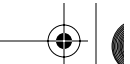






- 23.4.3 The NRL Taxonomy ..... 671
  - 23.4.3.1 *The Flaw Classes* ..... 671
  - 23.4.3.2 *Legacy* ..... 672
- 23.4.4 Aslam's Model ..... 673
  - 23.4.4.1 *The Flaw Classes* ..... 673
  - 23.4.4.2 *Legacy* ..... 673
- 23.4.5 Comparison and Analysis ..... 674
  - 23.4.5.1 *The xterm Log File Flaw* ..... 674
  - 23.4.5.2 *The fingerd Buffer Overflow Flaw* ..... 676
  - 23.4.5.3 *Summary* ..... 678
- 23.5 Gupta and Gligor's Theory of Penetration Analysis ..... 678
  - 23.5.1 The Flow-Based Model of Penetration Analysis ..... 679
  - 23.5.2 The Automated Penetration Analysis Tool ..... 682
  - 23.5.3 Discussion ..... 682
- 23.6 Summary ..... 683
- 23.7 Research Issues ..... 683
- 23.8 Further Reading ..... 684
- 23.9 Exercises ..... 685
  
- Chapter 24 Auditing ..... 689**
  - 24.1 Definitions ..... 689
  - 24.2 Anatomy of an Auditing System ..... 690
    - 24.2.1 Logger ..... 690
    - 24.2.2 Analyzer ..... 692
    - 24.2.3 Notifier ..... 693
  - 24.3 Designing an Auditing System ..... 693
    - 24.3.1 Implementation Considerations ..... 696
    - 24.3.2 Syntactic Issues ..... 696
    - 24.3.3 Log Sanitization ..... 698
    - 24.3.4 Application and System Logging ..... 700
  - 24.4 A Posteriori Design ..... 701
    - 24.4.1 Auditing to Detect Violations of a Known Policy ..... 702
      - 24.4.1.1 *State-Based Auditing* ..... 702
      - 24.4.1.2 *Transition-Based Auditing* ..... 703
    - 24.4.2 Auditing to Detect Known Violations of a Policy ..... 704
  - 24.5 Auditing Mechanisms ..... 705
    - 24.5.1 Secure Systems ..... 706
    - 24.5.2 Nonsecure Systems ..... 707
  - 24.6 Examples: Auditing File Systems ..... 708
    - 24.6.1 Audit Analysis of the NFS Version 2 Protocol ..... 709
    - 24.6.2 The Logging and Auditing File System (LAFS) ..... 713
    - 24.6.3 Comparison ..... 714





xxii Contents

24.7 Audit Browsing ..... 715  
24.8 Summary ..... 718  
24.9 Research Issues ..... 718  
24.10 Further Reading ..... 719  
24.11 Exercises ..... 720

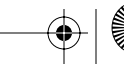
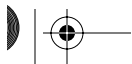
**Chapter 25 Intrusion Detection ..... 723**

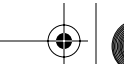
25.1 Principles ..... 723  
25.2 Basic Intrusion Detection ..... 724  
25.3 Models ..... 727  
    25.3.1 Anomaly Modeling ..... 727  
        25.3.1.1 Derivation of Statistics ..... 730  
    25.3.2 Misuse Modeling ..... 733  
    25.3.3 Specification Modeling ..... 738  
    25.3.4 Summary ..... 740  
25.4 Architecture ..... 742  
    25.4.1 Agent ..... 742  
        25.4.1.1 Host-Based Information Gathering ..... 744  
        25.4.1.2 Network-Based Information Gathering ..... 744  
        25.4.1.3 Combining Sources ..... 745  
    25.4.2 Director ..... 746  
    25.4.3 Notifier ..... 747  
25.5 Organization of Intrusion Detection Systems ..... 748  
    25.5.1 Monitoring Network Traffic for Intrusions: NSM ..... 749  
    25.5.2 Combining Host and Network Monitoring: DIDS ..... 750  
    25.5.3 Autonomous Agents: AAFID ..... 752  
25.6 Intrusion Response ..... 754  
    25.6.1 Incident Prevention ..... 754  
    25.6.2 Intrusion Handling ..... 755  
        25.6.2.1 Containment Phase ..... 756  
        25.6.2.2 Eradication Phase ..... 757  
        25.6.2.3 Follow-Up Phase ..... 760  
25.7 Summary ..... 765  
25.8 Research Issues ..... 765  
25.9 Further Reading ..... 767  
25.10 Exercises ..... 767

**PART 8: PRACTICUM ..... 771**

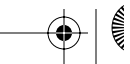
**Chapter 26 Network Security ..... 773**

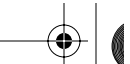
26.1 Introduction ..... 773





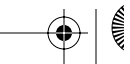
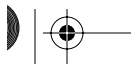
26.2	Policy Development	774
26.2.1	Data Classes	775
26.2.2	User Classes	776
26.2.3	Availability	778
26.2.4	Consistency Check	778
26.3	Network Organization	779
26.3.1	Firewalls and Proxies	780
26.3.2	Analysis of the Network Infrastructure	782
26.3.2.1	Outer Firewall Configuration	783
26.3.2.2	Inner Firewall Configuration	785
26.3.3	In the DMZ	786
26.3.3.1	DMZ Mail Server	786
26.3.3.2	DMZ WWW Server	787
26.3.3.3	DMZ DNS Server	789
26.3.3.4	DMZ Log Server	789
26.3.3.5	Summary	790
26.3.4	In the Internal Network	790
26.3.5	General Comment on Assurance	792
26.4	Availability and Network Flooding	793
26.4.1	Intermediate Hosts	793
26.4.2	TCP State and Memory Allocations	794
26.5	Anticipating Attacks	796
26.6	Summary	798
26.7	Research Issues	798
26.8	Further Reading	799
26.9	Exercises	799
<b>Chapter 27 System Security</b>		<b>805</b>
27.1	Introduction	805
27.2	Policy	806
27.2.1	The Web Server System in the DMZ	806
27.2.2	The Development System	807
27.2.3	Comparison	810
27.2.4	Conclusion	811
27.3	Networks	811
27.3.1	The Web Server System in the DMZ	812
27.3.2	The Development System	814
27.3.3	Comparison	816
27.4	Users	817
27.4.1	The Web Server System in the DMZ	817
27.4.2	The Development System	819
27.4.3	Comparison	822



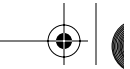


xxiv Contents

27.5	Authentication .....	822
27.5.1	The Web Server System in the DMZ .....	823
27.5.2	Development Network System .....	823
27.5.3	Comparison .....	825
27.6	Processes .....	825
27.6.1	The Web Server System in the DMZ .....	825
27.6.2	The Development System .....	829
27.6.3	Comparison .....	830
27.7	Files .....	831
27.7.1	The Web Server System in the DMZ .....	831
27.7.2	The Development System .....	833
27.7.3	Comparison .....	835
27.8	Retrospective .....	837
27.8.1	The Web Server System in the DMZ .....	837
27.8.2	The Development System .....	838
27.9	Summary .....	838
27.10	Research Issues .....	839
27.11	Further Reading .....	840
27.12	Exercises .....	840
	<b>Chapter 28 User Security .....</b>	<b>845</b>
28.1	Policy .....	845
28.2	Access .....	846
28.2.1	Passwords .....	846
28.2.2	The Login Procedure .....	848
28.2.2.1	<i>Trusted Hosts</i> .....	850
28.2.3	Leaving the System .....	850
28.3	Files and Devices .....	852
28.3.1	Files .....	852
28.3.1.1	<i>File Permissions on Creation</i> .....	853
28.3.1.2	<i>Group Access</i> .....	854
28.3.1.3	<i>File Deletion</i> .....	855
28.3.2	Devices .....	857
28.3.2.1	<i>Writable Devices</i> .....	857
28.3.2.2	<i>Smart Terminals</i> .....	857
28.3.2.3	<i>Monitors and Window Systems</i> .....	859
28.4	Processes .....	860
28.4.1	Copying and Moving Files .....	860
28.4.2	Accidentally Overwriting Files .....	861
28.4.3	Encryption, Cryptographic Keys, and Passwords .....	861
28.4.4	Start-up Settings .....	863



- 28.4.5 Limiting Privileges . . . . . 863
- 28.4.6 Malicious Logic . . . . . 864
- 28.5 Electronic Communications . . . . . 865
  - 28.5.1 Automated Electronic Mail Processing . . . . . 865
  - 28.5.2 Failure to Check Certificates . . . . . 865
  - 28.5.3 Sending Unexpected Content . . . . . 866
- 28.6 Summary . . . . . 866
- 28.7 Research Issues . . . . . 867
- 28.8 Further Reading . . . . . 867
- 28.9 Exercises . . . . . 868
  
- Chapter 29 Program Security . . . . . 869**
- 29.1 Introduction . . . . . 869
- 29.2 Requirements and Policy . . . . . 870
  - 29.2.1 Requirements . . . . . 870
  - 29.2.2 Threats . . . . . 871
    - 29.2.2.1 *Group 1: Unauthorized Users*  
*Accessing Role Accounts* . . . . . 871
    - 29.2.2.1 *Group 2: Authorized Users*  
*Accessing Role Accounts* . . . . . 872
    - 29.2.2.1 *Summary* . . . . . 873
- 29.3 Design . . . . . 873
  - 29.3.1 Framework . . . . . 874
    - 29.3.1.1 *User Interface* . . . . . 874
    - 29.3.1.2 *High-Level Design* . . . . . 874
  - 29.3.2 Access to Roles and Commands . . . . . 875
    - 29.3.2.1 *Interface* . . . . . 876
    - 29.3.2.2 *Internals* . . . . . 876
    - 29.3.2.3 *Storage of the Access Control Data* . . . . . 877
- 29.4 Refinement and Implementation . . . . . 880
  - 29.4.1 First-Level Refinement. . . . . 880
  - 29.4.2 Second-Level Refinement . . . . . 881
  - 29.4.3 Functions . . . . . 884
    - 29.4.3.1 *Obtaining Location* . . . . . 884
    - 29.4.3.2 *The Access Control Record* . . . . . 885
    - 29.4.3.3 *Error Handling in the Reading and Matching Routines* 886
  - 29.4.4 Summary . . . . . 887
- 29.5 Common Security-Related Programming Problems . . . . . 887
  - 29.5.1 Improper Choice of Initial Protection Domain. . . . . 888
    - 29.5.1.1 *Process Privileges* . . . . . 888
    - 29.5.1.1 *Access Control File Permissions* . . . . . 890

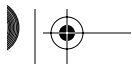


xxvi Contents

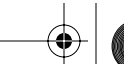
- 29.5.1.3 *Memory Protection* . . . . . 891
- 29.5.1.4 *Trust in the System* . . . . . 892
- 29.5.2 Improper Isolation of Implementation Detail . . . . . 893
  - 29.5.2.1 *Resource Exhaustion and User Identifiers* . . . . . 893
  - 29.5.2.2 *Validating the Access Control Entries* . . . . . 894
  - 29.5.2.3 *Restricting the Protection Domain of the Role Process* 894
- 29.5.3 Improper Change . . . . . 895
  - 29.5.3.1 *Memory* . . . . . 895
  - 29.5.3.2 *Changes in File Contents* . . . . . 898
  - 29.5.3.3 *Race Conditions in File Accesses* . . . . . 898
- 29.5.4 Improper Naming . . . . . 899
- 29.5.5 Improper Deallocation or Deletion . . . . . 901
- 29.5.6 Improper Validation . . . . . 902
  - 29.5.6.1 *Bounds Checking* . . . . . 902
  - 29.5.6.2 *Type Checking*. . . . . 903
  - 29.5.6.3 *Error Checking* . . . . . 904
  - 29.5.6.4 *Checking for Valid, not Invalid, Data*. . . . . 904
  - 29.5.6.5 *Checking Input* . . . . . 905
  - 29.5.6.6 *Designing for Validation*. . . . . 907
- 29.5.7 Improper Indivisibility. . . . . 907
- 29.5.8 Improper Sequencing. . . . . 908
- 29.5.9 Improper Choice of Operand or Operation . . . . . 909
- 29.5.10 Summary . . . . . 911
- 29.6 Testing, Maintenance, and Operation . . . . . 913
  - 29.6.1 Testing . . . . . 913
    - 29.6.1.1 *Testing the Module* . . . . . 914
  - 29.6.2 Testing Composed Modules . . . . . 916
  - 29.6.3 Testing the Program . . . . . 917
- 29.7 Distribution . . . . . 917
- 29.8 Conclusion . . . . . 918
- 29.9 Summary . . . . . 919
- 29.10 Research Issues . . . . . 919
- 29.11 Further Reading . . . . . 919
- 29.12 Exercises . . . . . 920

**PART 9: END MATTER 923**

- Chapter 30 Lattices . . . . . 925**
  - 30.1 Basics . . . . . 925
  - 30.2 Lattices . . . . . 926
  - 30.3 Exercises . . . . . 927



<b>Chapter 31 The Extended Euclidean Algorithm</b> .....	<b>929</b>
31.1 The Euclidean Algorithm .....	929
31.2 The Extended Euclidean Algorithm .....	930
31.3 Solving $ax \bmod n = 1$ .....	932
31.4 Solving $ax \bmod n = b$ .....	932
31.5 Exercises .....	933
<b>Chapter 32 Entropy and Uncertainty</b> .....	<b>935</b>
32.1 Conditional and Joint Probability .....	935
32.2 Entropy and Uncertainty .....	937
32.3 Joint and Conditional Entropy .....	938
32.3.1 Joint Entropy .....	938
32.3.2 Conditional Entropy .....	939
32.3.3 Perfect Secrecy .....	940
32.4 Exercises .....	940
<b>Chapter 33 Virtual Machines</b> .....	<b>941</b>
33.1 Virtual Machine Structure .....	941
33.2 Virtual Machine Monitor .....	942
33.2.1 Privilege and Virtual Machines .....	943
33.2.2 Physical Resources and Virtual Machines .....	944
33.2.3 Paging and Virtual Machines .....	945
33.3 Exercises .....	946
<b>Chapter 34 Symbolic Logic</b> .....	<b>947</b>
34.1 Propositional Logic .....	947
34.1.1 Natural Deduction in Propositional Logic .....	948
34.1.1.1 Rules .....	949
34.1.1.2 Derived Rules .....	950
34.1.2 Well-Formed Formulas .....	950
34.1.3 Truth Tables .....	950
34.1.4 Mathematical Induction .....	951
34.2 Predicate Logic .....	952
34.2.1 Natural Deduction in Predicate Logic .....	953
34.3 Temporal Logic Systems .....	954
34.3.1 Syntax of CTL .....	954
34.3.2 Semantics of CTL .....	955
34.4 Exercises .....	956
<b>Chapter 35 Example Academic Security Policy</b> .....	<b>959</b>
35.1 University of California E-mail Policy .....	959



xxviii Contents

35.1.1	Summary: E-mail Policy Highlights	959
35.1.1.1	<i>Cautions</i>	959
35.1.1.2	<i>Do</i>	960
35.1.1.3	<i>Do Not</i>	961
35.1.1.4	<i>Does This Policy Apply to You?</i>	961
35.1.2	University of California Electronic Mail Policy	961
35.1.2.1	<i>Introduction</i>	961
35.1.2.2	<i>Purpose</i>	963
35.1.2.3	<i>Definitions</i>	963
35.1.2.4	<i>Scope</i>	964
35.1.2.5	<i>General Provisions</i>	965
35.1.2.6	<i>Specific Provisions</i>	967
35.1.2.7	<i>Policy Violations</i>	971
35.1.2.8	<i>Responsibility for Policy</i>	971
35.1.2.9	<i>Campus Responsibilities and Discretion</i>	971
35.1.2.10	<i>Appendix A—Definitions</i>	972
35.1.2.11	<i>Appendix B—References</i>	975
35.1.2.12	<i>Appendix C—Policies Relating to Nonconsensual Access</i>	976
35.1.3	UC Davis Implementation of the Electronic Mail Policy	977
35.1.3.1	<i>Purpose and Scope</i>	978
35.1.3.2	<i>Definitions</i>	978
35.1.3.3	<i>Policy</i>	978
35.1.4	References and Related Policy	988
35.2	The Acceptable Use Policy for the University of California, Davis	989
35.2.1	Part I	989
35.2.1.1	<i>Introduction</i>	989
35.2.1.2	<i>Rights and Responsibilities</i>	989
35.2.1.3	<i>Existing Legal Context</i>	989
35.2.1.4	<i>Enforcement</i>	990
35.2.2	Part 2	990
	<b>Bibliography</b>	<b>993</b>
	<b>Index</b>	<b>1063</b>

