- Preface p. xxxi
- Goals p. xxxii
- Philosophy p. xxxiii
- Organization p. xxxv
- Roadmap p. xxxvi
- Dependencies p. xxxvi
- Background p. xxxvii
- Undergraduate Level p. xxxviii
- Graduate Level p. xxxviii
- Practitioners p. xl
- Special Acknowledgment p. xl
- Acknowledgments p. xl
- Part 1 Introduction p. 1
- Chapter 1 An Overview of Computer Security p. 3
- 1.1 The Basic Components p. 3
- 1.2 Threats p. 6
- 1.3 Policy and Mechanism p. 9
- 1.4 Assumptions and Trust p. 11
- 1.5 Assurance p. 12
- 1.6 Operational Issues p. 16
- 1.7 Human Issues p. 19
- 1.8 Tying It All Together p. 22
- 1.9 Summary p. 23
- 1.10 Research Issues p. 24
- 1.11 Further Reading p. 24
- 1.12 Exercises p. 25
- Part 2 Foundations p. 29
- Chapter 2 Access Control Matrix p. 31
- 2.1 Protection State p. 31
- 2.2 Access Control Matrix Model p. 32
- 2.3 Protection State Transitions p. 37
- 2.4 Copying, Owning, and the Attenuation of Privilege p. 41
- 2.5 Summary p. 43
- 2.6 Research Issues p. 44
- 2.7 Further Reading p. 44
- 2.8 Exercises p. 44
- Chapter 3 Foundational Results p. 47
- 3.1 The General Question p. 47
- 3.2 Basic Results p. 48
- 3.3 The Take-Grant Protection Model p. 53
- 3.4 Closing the Gap p. 65
- 3.5 Expressive Power and the Models p. 78
- 3.6 Summary p. 90
- 3.7 Research Issues p. 90

- 3.8 Further Reading p. 91
- 3.9 Exercises p. 91
- Part 3 Policy p. 93
- Chapter 4 Security Policies p. 95
- 4.1 Security Policies p. 95
- 4.2 Types of Security Policies p. 99
- 4.3 The Role of Trust p. 101
- 4.4 Types of Access Control p. 103
- 4.5 Policy Languages p. 104
- 4.6 Example: Academic Computer Security Policy p. 111
- 4.7 Security and Precision p. 114
- 4.8 Summary p. 119
- 4.9 Research Issues p. 119
- 4.10 Further Reading p. 120
- 4.11 Exercises p. 120
- Chapter 5 Confidentiality Policies p. 123
- 5.1 Goals of Confidentiality Policies p. 123
- 5.2 The Bell-LaPadula Model p. 124
- 5.3 Tranquility p. 142
- 5.4 The Controversy over the Bell-LaPadula Model p. 143
- 5.5 Summary p. 148
- 5.6 Research Issues p. 148
- 5.7 Further Reading p. 149
- 5.8 Exercises p. 150
- Chapter 6 Integrity Policies p. 151
- 6.1 Goals p. 151
- 6.2 Biba Integrity Model p. 153
- 6.3 Lipner's Integrity Matrix Model p. 156
- 6.4 Clark-Wilson Integrity Model p. 160
- 6.5 Summary p. 166
- 6.6 Research Issues p. 166
- 6.7 Further Reading p. 167
- 6.8 Exercises p. 167
- Chapter 7 Hybrid Policies p. 169
- 7.1 Chinese Wall Model p. 169
- 7.2 Clinical Information Systems Security Policy p. 177
- 7.3 Originator Controlled Access Control p. 180
- 7.4 Role-Based Access Control p. 182
- 7.5 Summary p. 184
- 7.6 Research Issues p. 184
- 7.7 Further Reading p. 184
- 7.8 Exercises p. 185
- Chapter 8 Noninterference and Policy Composition p. 187
- 8.1 The Problem p. 187

- 8.2 Deterministic Noninterference p. 191
- 8.3 Nondeducibility p. 202
- 8.4 Generalized Noninterference p. 205
- 8.5 Restrictiveness p. 208
- 8.6 Summary p. 210
- 8.7 Research Issues p. 211
- 8.8 Further Reading p. 211
- 8.9 Exercises p. 212
- Part 4 Implementation I: Cryptography p. 215
- Chapter 9 Basic Cryptography p. 217
- 9.1 What Is Cryptography? p. 217
- 9.2 Classical Cryptosystems p. 218
- 9.3 Public Key Cryptography p. 233
- 9.4 Cryptographic Checksums p. 237
- 9.5 Summary p. 239
- 9.6 Research Issues p. 240
- 9.7 Further Reading p. 240
- 9.8 Exercises p. 241
- Chapter 10 Key Management p. 245
- 10.1 Session and Interchange Keys p. 246
- 10.2 Key Exchange p. 246
- 10.3 Key Generation p. 252
- 10.4 Cryptographic Key Infrastructures p. 254
- 10.5 Storing and Revoking Keys p. 261
- 10.6 Digital Signatures p. 266
- 10.7 Summary p. 270
- 10.8 Research Issues p. 271
- 10.9 Further Reading p. 272
- 10.10 Exercises p. 272
- Chapter 11 Cipher Techniques p. 275
- 11.1 Problems p. 275
- 11.2 Stream and Block Ciphers p. 277
- 11.3 Networks and Cryptography p. 283
- 11.4 Example Protocols p. 286
- 11.5 Summary p. 306
- 11.6 Research Issues p. 306
- 11.7 Further Reading p. 306
- 11.8 Exercises p. 307
- Chapter 12 Authentication p. 309
- 12.1 Authentication Basics p. 309
- 12.2 Passwords p. 310
- 12.3 Challenge-Response p. 324
- 12.4 Biometrics p. 328
- 12.5 Location p. 331

- 12.6 Multiple Methods p. 331
- 12.7 Summary p. 333
- 12.8 Research Issues p. 334
- 12.9 Further Reading p. 335
- 12.10 Exercises p. 335
- Part 5 Implementation II: Systems p. 339
- Chapter 13 Design Principles p. 341
- 13.1 Overview p. 341
- 13.2 Design Principles p. 343
- 13.3 Summary p. 349
- 13.4 Research Issues p. 350
- 13.5 Further Reading p. 350
- 13.6 Exercises p. 351
- Chapter 14 Representing Identity p. 353
- 14.1 What Is Identity? p. 353
- 14.2 Files and Objects p. 354
- 14.3 Users p. 355
- 14.4 Groups and Roles p. 356
- 14.5 Naming and Certificates p. 357
- 14.6 Identity on the Web p. 366
- 14.7 Summary p. 377
- 14.8 Research Issues p. 378
- 14.9 Further Reading p. 378
- 14.10 Exercises p. 379
- Chapter 15 Access Control Mechanisms p. 381
- 15.1 Access Control Lists p. 381
- 15.2 Capabilities p. 390
- 15.3 Locks and Keys p. 396
- 15.4 Ring-Based Access Control p. 400
- 15.5 Propagated Access Control Lists p. 402
- 15.6 Summary p. 404
- 15.7 Research Issues p. 404
- 15.8 Further Reading p. 405
- 15.9 Exercises p. 405
- Chapter 16 Information Flow p. 407
- 16.1 Basics and Background p. 407
- 16.2 Nonlattice Information Flow Policies p. 410
- 16.3 Compiler-Based Mechanisms p. 415
- 16.4 Execution-Based Mechanisms p. 429
- 16.5 Example Information Flow Controls p. 433
- 16.6 Summary p. 436
- 16.7 Research Issues p. 436
- 16.8 Further Reading p. 437
- 16.9 Exercises p. 437

- Chapter 17 Confinement Problem p. 439
- 17.1 The Confinement Problem p. 439
- 17.2 Isolation p. 442
- 17.3 Covert Channels p. 446
- 17.4 Summary p. 470
- 17.5 Research Issues p. 471
- 17.6 Further Reading p. 472
- 17.7 Exercises p. 472
- Part 6 Assurance p. 475
- Chapter 18 Introduction to Assurance p. 477
- 18.1 Assurance and Trust p. 477
- 18.2 Building Secure and Trusted Systems p. 484
- 18.3 Summary p. 492
- 18.4 Research Issues p. 493
- 18.5 Further Reading p. 494
- 18.6 Exercises p. 494
- Chapter 19 Building Systems with Assurance p. 497
- 19.1 Assurance in Requirements Definition and Analysis p. 497
- 19.2 Assurance During System and Software Design p. 510
- 19.3 Assurance in Implementation and Integration p. 531
- 19.4 Assurance During Operation and Maintenance p. 541
- 19.5 Summary p. 541
- 19.6 Research Issues p. 542
- 19.7 Further Reading p. 542
- 19.8 Exercises p. 543
- Chapter 20 Formal Methods p. 545
- 20.1 Formal Verification Techniques p. 545
- 20.2 Formal Specification p. 548
- 20.3 Early Formal Verification Techniques p. 551
- 20.4 Current Verification Systems p. 559
- 20.5 Summary p. 567
- 20.6 Research Issues p. 568
- 20.7 Further Reading p. 568
- 20.8 Exercises p. 569
- Chapter 21 Evaluating Systems p. 571
- 21.1 Goals of Formal Evaluation p. 571
- 21.2 TCSEC: 1983-1999 p. 574
- 21.3 International Efforts and the ITSEC: 1991-2001 p. 581
- 21.4 Commercial International Security Requirements: 1991 p. 586
- 21.5 Other Commercial Efforts: Early 1990s p. 587
- 21.6 The Federal Criteria: 1992 p. 587
- 21.7 FIPS 140: 1994-Present p. 589
- 21.8 The Common Criteria: 1998-Present p. 591
- 21.9 SSE-CMM: 1997-Present p. 604

- 21.10 Summary p. 607
- 21.11 Research Issues p. 608
- 21.12 Further Reading p. 608
- 21.13 Exercises p. 609
- Part 7 Special Topics p. 611
- Chapter 22 Malicious Logic p. 613
- 22.1 Introduction p. 613
- 22.2 Trojan Horses p. 614
- 22.3 Computer Viruses p. 615
- 22.4 Computer Worms p. 623
- 22.5 Other Forms of Malicious Logic p. 624
- 22.6 Theory of Malicious Logic p. 626
- 22.7 Defenses p. 630
- 22.8 Summary p. 640
- 22.9 Research Issues p. 640
- 22.10 Further Reading p. 641
- 22.11 Exercises p. 642
- Chapter 23 Vulnerability Analysis p. 645
- 23.1 Introduction p. 645
- 23.2 Penetration Studies p. 647
- 23.3 Vulnerability Classification p. 660
- 23.4 Frameworks p. 662
- 23.5 Gupta and Gligor's Theory of Penetration Analysis p. 678
- 23.6 Summary p. 683
- 23.7 Research Issues p. 683
- 23.8 Further Reading p. 684
- 23.9 Exercises p. 685
- Chapter 24 Auditing p. 689
- 24.1 Definitions p. 689
- 24.2 Anatomy of an Auditing System p. 690
- 24.3 Designing an Auditing System p. 693
- 24.4 A Posteriori Design p. 701
- 24.5 Auditing Mechanisms p. 705
- 24.6 Examples: Auditing File Systems p. 708
- 24.7 Audit Browsing p. 715
- 24.8 Summary p. 718
- 24.9 Research Issues p. 718
- 24.10 Further Reading p. 719
- 24.11 Exercises p. 720
- Chapter 25 Intrusion Detection p. 723
- 25.1 Principles p. 723
- 25.2 Basic Intrusion Detection p. 724
- 25.3 Models p. 727
- 25.4 Architecture p. 742

- 25.5 Organization of Intrusion Detection Systems p. 748
- 25.6 Intrusion Response p. 754
- 25.7 Summary p. 765
- 25.8 Research Issues p. 765
- 25.9 Further Reading p. 767
- 25.10 Exercises p. 767
- Part 8 Practicum p. 771
- Chapter 26 Network Security p. 773
- 26.1 Introduction p. 773
- 26.2 Policy Development p. 774
- 26.3 Network Organization p. 779
- 26.4 Availability and Network Flooding p. 793
- 26.5 Anticipating Attacks p. 796
- 26.6 Summary p. 798
- 26.7 Research Issues p. 798
- 26.8 Further Reading p. 799
- 26.9 Exercises p. 799
- Chapter 27 System Security p. 805
- 27.1 Introduction p. 805
- 27.2 Policy p. 806
- 27.3 Networks p. 811
- 27.4 Users p. 817
- 27.5 Authentication p. 822
- 27.6 Processes p. 825
- 27.7 Files p. 831
- 27.8 Retrospective p. 837
- 27.9 Summary p. 838
- 27.10 Research Issues p. 839
- 27.11 Further Reading p. 840
- 27.12 Exercises p. 840
- Chapter 28 User Security p. 845
- 28.1 Policy p. 845
- 28.2 Access p. 846
- 28.3 Files and Devices p. 852
- 28.4 Processes p. 860
- 28.5 Electronic Communications p. 865
- 28.6 Summary p. 866
- 28.7 Research Issues p. 867
- 28.8 Further Reading p. 867
- 28.9 Exercises p. 868
- Chapter 29 Program Security p. 869
- 29.1 Introduction p. 869
- 29.2 Requirements and Policy p. 870
- 29.3 Design p. 873

- 29.4 Refinement and Implementation p. 880
- 29.5 Common Security-Related Programming Problems p. 887
- 29.6 Testing, Maintenance, and Operation p. 913
- 29.7 Distribution p. 917
- 29.8 Conclusion p. 919
- 29.9 Summary p. 919
- 29.10 Research Issues p. 919
- 29.11 Further Reading p. 920
- 29.12 Exercises p. 920
- Part 9 End Matter p. 923
- Chapter 30 Lattices p. 925
- 30.1 Basics p. 925
- 30.2 Lattices p. 926
- 30.3 Exercises p. 927
- Chapter 31 The Extended Euclidean Algorithm p. 929
- 31.1 The Euclidean Algorithm p. 929
- 31.2 The Extended Euclidean Algorithm p. 930
- 31.3 Solving ax mod n = 1 p. 932
- 31.4 Solving ax mod n = b p. 932
- 31.5 Exercises p. 933
- Chapter 32 Entropy and Uncertainty p. 935
- 32.1 Conditional and Joint Probability p. 935
- 32.2 Entropy and Uncertainty p. 937
- 32.3 Joint and Conditional Entropy p. 938
- 32.4 Exercises p. 940
- Chapter 33 Virtual Machines p. 941
- 33.1 Virtual Machine Structure p. 941
- 33.2 Virtual Machine Monitor p. 942
- 33.3 Exercises p. 946
- Chapter 34 Symbolic Logic p. 947
- 34.1 Propositional Logic p. 947
- 34.2 Predicate Logic p. 952
- 34.3 Temporal Logic Systems p. 954
- 34.4 Exercises p. 956
- Chapter 35 Example Academic Security Policy p. 959
- 35.1 University of California E-mail Policy p. 959
- 35.2 The Acceptable Use Policy for the University of California, Davis p. 989
- Bibliography p. 993
- Index p. 1063