Preface xxix
Acknowledgments xlv
About the Author xlix
Part I: Introduction 1
Chapter 1: An Overview of Computer Security 3
1.1 The Basic Components 3
1.2 Threats 6
1.3 Policy and Mechanism 9
1.4 Assumptions and Trust 11
1.5 Assurance 12
1.6 Operational Issues 16
1.7 Human Issues 20
1.8 Tying It All Together 22
1.9 Summary 24
1.10 Research Issues 24
1.11 Further Reading 25
1.12 Exercises 25
Part II: Foundations 29
Chapter 2: Access Control Matrix 31
2.1 Protection State 31
2.2 Access Control Matrix Model 32
2.3 Protection State Transitions 37
2.4 Copying, Owning, and the Attenuation of Privilege 42
2.5 Summary 44
2.6 Research Issues 44
2.7 Further Reading 44
2.8 Exercises 45
Chapter 3: Foundational Results 49
3.1 The General Question 49
3.2 Basic Results 51
3.3 The Take-Grant Protection Model 56
3.4 Closing the Gap: The Schematic Protection Model 68
3.5 Expressive Power and the Models 81
3.6 Comparing Security Properties of Models 94
3.7 Summary 101
3.8 Research Issues 102
3.9 Further Reading 102
3.10 Exercises 103
Part III: Policy 107
Chapter 4: Security Policies 109
4.1 The Nature of Security Policies 109
4.2 Types of Security Policies 113
4.3 The Role of Trust 115
4.4 Types of Access Control 117
4.5 Policy Languages 118
4.6 Example: Academic Computer Security Policy 126
4.7 Security and Precision 131
4.8 Summary 136

4.9 Research Issues 136
4.10 Further Reading 137
4.11 Exercises 138
Chapter 5: Confidentiality Policies 141
5.1 Goals of Confidentiality Policies 141
5.2 The Bell-LaPadula Model 142
5.3 Tranquility 161
5.4 The Controversy over the Bell-LaPadula Model 164
5.5 Summary 169
5.6 Research Issues 169
5.7 Further Reading 170
5.8 Exercises 171
Chapter 6: Integrity Policies 173
6.1 Goals 173
6.2 The Biba Model 175
6.3 Lipner's Integrity Matrix Model 178
6.4 Clark-Wilson Integrity Model 183
6.5 Trust Models 189
6.6 Summary 196
6.7 Research Issues 196
6.8 Further Reading 197
6.9 Exercises 198
Chapter 7: Availability Policies 201
7.1 Goals of Availability Policies 201
7.2 Deadlock 202
7.3 Denial of Service Models 203
7.4 Example: Availability and Network Flooding 215
7.5 Summary 222
7.6 Research Issues 222
7.7 Further Reading 223
7.8 Exercises 224
Chapter 8: Hybrid Policies 227
8.1 Chinese Wall Model 227
8.2 Clinical Information Systems Security Policy 236
8.3 Originator Controlled Access Control 239
8.4 Role-Based Access Control 244
8.5 Break-the-Glass Policies 249
8.6 Summary 250
8.7 Research Issues 250
8.8 Further Reading 251
8.9 Exercises 252
Chapter 9: Noninterference and Policy Composition 255
9.1 The Problem 255
9.2 Deterministic Noninterference 259
9.3 Nondeducibility 271
9.4 Generalized Noninterference 274
9.5 Restrictiveness 277
9.6 Side Channels and Deducibility 280

9.7 Summary 282
9.8 Research Issues 283
9.9 Further Reading 283
9.10 Exercises 285
Part IV: Implementation I: Cryptography 287
Chapter 10: Basic Cryptography 289
10.1 Cryptography 289
10.2 Symmetric Cryptosystems 291
10.3 Public Key Cryptography 306
10.4 Cryptographic Checksums 315
10.5 Digital Signatures 318
10.6 Summary 323
10.7 Research Issues 324
10.8 Further Reading 325
10.9 Exercises 326
Chapter 11: Key Management 331
11.1 Session and Interchange Keys 332
11.2 Key Exchange 332
11.3 Key Generation 341
11.4 Cryptographic Key Infrastructures 343
11.5 Storing and Revoking Keys 353
11.6 Summary 359
11.7 Research Issues 360
11.8 Further Reading 361
11.9 Exercises 362
Chapter 12: Cipher Techniques 367
12.1 Problems 367
12.2 Stream and Block Ciphers 370
12.3 Authenticated Encryption 377
12.4 Networks and Cryptography 381
12.5 Example Protocols 384
12.6 Summary 410
12.7 Research Issues 411
12.8 Further Reading 411
12.9 Exercises 413
Chapter 13: Authentication 415
13.1 Authentication Basics 415
13.2 Passwords 416
13.3 Password Selection 418
13.4 Attacking Passwords 426
13.5 Password Aging 434
13.6 Challenge-Response 438
13.7 Biometrics 441
13.8 Location 445
13.9 Multifactor Authentication 446
13.10 Summary 448
13.11 Research Issues 449
13.12 Further Reading 450

13.13 Exercises 451
Part V: Implementation II: Systems 453
Chapter 14: Design Principles 455
14.1 Underlying Ideas 455
14.2 Principles of Secure Design 457
14.3 Summary 466
14.4 Research Issues 466
14.5 Further Reading 467
14.6 Exercises 468
Chapter 15: Representing Identity 471
15.1 What Is Identity? 471
15.2 Files and Objects 472
15.3 Users 473
15.4 Groups and Roles 475
15.5 Naming and Certificates 476
15.6 Identity on the Web 484
15.7 Anonymity on the Web 490
15.8 Summary 501
15.9 Research Issues 502
15.10 Further Reading 503
15.11 Exercises 504
Chapter 16: Access Control Mechanisms 507
16.1 Access Control Lists 507
16.2 Capabilities 518
16.3 Locks and Keys 526
16.4 Ring-Based Access Control 531
16.5 Propagated Access Control Lists 533
16.6 Summary 535
16.7 Research Issues 535
16.8 Further Reading 536
16.9 Exercises 536
Chapter 17: Information Flow 539
17.1 Basics and Background 539
17.2 Nonlattice Information Flow Policies 542
17.3 Static Mechanisms 548
17.4 Dynamic Mechanisms 562
17.5 Integrity Mechanisms 566
17.6 Example Information Flow Controls 567
17.7 Summary 574
17.8 Research Issues 574
17.9 Further Reading 575
17.10 Exercises 576
Chapter 18: Confinement Problem 579
18.1 The Confinement Problem 579
18.2 Isolation 582
18.3 Covert Channels 594
18.4 Summary 619
18.5 Research Issues 620

18.6 Further Reading 620
18.7 Exercises 622
Part VI: Assurance 625
Contributed by Elisabeth Sullivan and Michelle Ruppel
Chapter 19: Introduction to Assurance 627
19.1 Assurance and Trust 627
19.2 Building Secure and Trusted Systems 634
19.3 Summary 645
19.4 Research Issues 645
19.5 Further Reading 646
19.6 Exercises 647
Chapter 20: Building Systems with Assurance 649
20.1 Assurance in Requirements Definition and Analysis 649
20.2 Assurance during System and Software Design 662
20.3 Assurance in Implementation and Integration 685
20.4 Assurance during Operation and Maintenance 695
20.5 Summary 696
20.6 Research Issues 696
20.7 Further Reading 697
20.8 Exercises 698
Chapter 21: Formal Methods 699
21.1 Formal Verification Techniques 699
21.2 Formal Specification 702
21.3 Early Formal Verification Techniques 705
21.4 Current Verification Systems 713
21.5 Functional Programming Languages 721
21.6 Formally Verified Products 722
21.7 Summary 723
21.8 Research Issues 724
21.9 Further Reading 725
21.10 Exercises 725
Chapter 22: Evaluating Systems 727
22.1 Goals of Formal Evaluation 727
22.2 TCSEC: 1983-1999 730
22.3 International Efforts and the ITSEC: 1991-2001 737
22.4 Commercial International Security Requirements: 1991 742
22.5 Other Commercial Efforts: Early 1990s 744
22.6 The Federal Criteria: 1992 744
22.7 FIPS 140: 1994-Present 746
22.8 The Common Criteria: 1998-Present 749
22.9 SSE-CMM: 1997-Present 765
22.10 Summary 768
22.11 Research Issues 769
22.12 Further Reading 769
22.13 Exercises 770
Part VII: Special Topics 773
Chapter 23: Malware 775
23.1 Introduction 775

23.2 Trojan Horses 776
23.3 Computer Viruses 780
23.4 Computer Worms 790
23.5 Bots and Botnets 793
23.6 Other Malware 796
23.7 Combinations 803
23.8 Theory of Computer Viruses 803
23.9 Defenses 808
23.10 Summary 820
23.11 Research Issues 820
23.12 Further Reading 821
23.13 Exercises 822
Chapter 24: Vulnerability Analysis 825
24.1 Introduction 825
24.2 Penetration Studies 827
24.3 Vulnerability Classification 845
24.4 Frameworks 849
24.5 Standards 864
24.6 Gupta and Gligor's Theory of Penetration Analysis 868
24.7 Summary 873
24.8 Research Issues 874
24.9 Further Reading 875
24.10 Exercises 876
Chapter 25: Auditing 879
25.1 Definition 879
25.2 Anatomy of an Auditing System 880
25.3 Designing an Auditing System 884
25.4 A Posteriori Design 893
25.5 Auditing Mechanisms 897
25.6 Examples: Auditing File Systems 900
25.7 Summary 910
25.8 Research Issues 911
25.9 Further Reading 912
25.10 Exercises 913
Chapter 26: Intrusion Detection 917
26.1 Principles 917
26.2 Basic Intrusion Detection 918
26.3 Models 920
26.4 Architecture 942
26.5 Organization of Intrusion Detection Systems 948
26.6 Summary 954
26.7 Research Issues 954
26.8 Further Reading 955
26.9 Exercises 956
Chapter 27: Attacks and Responses 959
27.1 Attacks 959
27.2 Representing Attacks 960
27.3 Intrusion Response 971

27.4 Digital Forensics 987
27.5 Summary 996
27.6 Research Issues 997
27.7 Further Reading 998
27.8 Exercises 999
Part VIII: Practicum 1003
Chapter 28: Network Security 1005
28.1 Introduction 1005
28.2 Policy Development 1006
28.3 Network Organization 1011
28.4 Availability 1026
28.5 Anticipating Attacks 1027
28.6 Summary 1028
28.7 Research Issues 1028
28.8 Further Reading 1029
28.9 Exercises 1030
Chapter 29: System Security 1035
29.1 Introduction 1035
29.2 Policy 1036
29.3 Networks 1042
29.4 Users 1048
29.5 Authentication 1053
29.6 Processes 1055
29.7 Files 1061
29.8 Retrospective 1066
29.9 Summary 1068
29.10 Research Issues 1068
29.11 Further Reading 1069
29.12 Exercises 1070
Chapter 30: User Security 1073
30.1 Policy 1073
30.2 Access 1074
30.3 Files and Devices 1080
30.4 Processes 1087
30.5 Electronic Communications 1092
30.6 Summary 1094
30.7 Research Issues 1095
30.8 Further Reading 1095
30.9 Exercises 1096
Chapter 31: Program Security 1099
31.1 Problem 1099
31.2 Requirements and Policy 1100
31.3 Design 1104
31.4 Refinement and Implementation 1111
31.5 Common Security-Related Programming Problems 1117
31.6 Testing, Maintenance, and Operation 1141
31.7 Distribution 1146
31.8 Summary 1147

31.9 Research Issues 1147
31.10 Further Reading 1148
31.11 Exercises 1148
Part IX: Appendices 1151
Appendix A: Lattices 1153
A.1 Basics 1153
A.2 Lattices 1154
A.3 Exercises 1155
Appendix B: The Extended Euclidean Algorithm 1157
B.1 The Euclidean Algorithm 1157
B.2 The Extended Euclidean Algorithm 1158
B.3 Solving $ax \bmod n = 1$ 1160
B.4 Solving $ax \bmod n = b$ 1161
B.5 Exercises 1161
Appendix C: Entropy and Uncertainty 1163
C.1 Conditional and Joint Probability 1163
C.2 Entropy and Uncertainty 1165
C.3 Joint and Conditional Entropy 1166
C.4 Exercises 1169
Appendix D: Virtual Machines 1171
D.1 Virtual Machine Structure 1171
D.2 Virtual Machine Monitor 1171
D.3 Exercises 1176
Appendix E: Symbolic Logic 1179
E.1 Propositional Logic 1179
E.2 Predicate Logic 1184
E.3 Temporal Logic Systems 1186
E.4 Exercises 1188
Appendix F: The Encryption Standards 1191
F.1 Data Encryption Standard 1191
F.2 Advanced Encryption Standard 1196
F.3 Exercises 1205
Appendix G: Example Academic Security Policy 1207
G.1 Acceptable Use Policy 1207
G.2 University of California Electronic Communications Policy 1212
G.3 User Advisories 1234
G.4 Electronic Communications—Allowable Use 1241
Appendix H: Programming Rules 1247
H.1 Implementation Rules 1247
H.2 Management Rules 1249
References 1251
Index 1341