

Computer Security

Art and Science

Second Edition

Matt Bishop

with contributions from

Elisabeth Sullivan and Michelle Ruppel

 Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Contents

Preface	xxix
Acknowledgments	xliv
About the Author	xlix

PART I : INTRODUCTION **1**

Chapter 1 An Overview of Computer Security	3
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	14
1.5.2 Design	14
1.5.3 Implementation	15
1.6 Operational Issues	16
1.6.1 Cost-Benefit Analysis	16
1.6.2 Risk Analysis	17
1.6.3 Laws and Customs	19
1.7 Human Issues	20
1.7.1 Organizational Problems	20
1.7.2 People Problems	21
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
2.2.1	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	42
2.4.1	Copy Right	42
2.4.2	Own Right	42
2.4.3	Principle of Attenuation of Privilege	43
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
3.3.1	Sharing of Rights	57
3.3.2	Interpretation of the Model	61
3.3.3	Theft in the Take-Grant Protection Model	62
3.3.4	Conspiracy	66
3.3.5	Summary	68
3.4	Closing the Gap: The Schematic Protection Model	68
3.4.1	Link Predicate	69
3.4.2	Filter Function	70
3.4.3	Putting It All Together	71
3.4.4	Demand and Create Operations	72
3.4.5	Safety Analysis	75
3.5	Expressive Power and the Models	81
3.5.1	Brief Comparison of HRU and SPM	82
3.5.2	Extending SPM	83
3.5.3	Simulation and Expressiveness	88
3.5.4	Typed Access Matrix Model	92
3.6	Comparing Security Properties of Models	94
3.6.1	Comparing Schemes and Security Properties	95
3.6.2	Augmented Typed Access Matrix Model	99

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
4.5.1	High-Level Policy Languages	119
4.5.2	Low-Level Policy Languages	125
4.6	Example: Academic Computer Security Policy	126
4.6.1	General University Electronic Communications Policy	127
4.6.2	Implementation at UC Davis	130
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
5.2.1	Informal Description	142
5.2.2	Example: Trusted Solaris	146
5.2.3	Formal Model	151
5.2.4	Example Model Instantiation: Multics	158
5.3	Tranquility	161
5.3.1	Declassification Principles	163
5.4	The Controversy over the Bell-LaPadula Model	164
5.4.1	McLean's \dagger -Property and the Basic Security Theorem	164
5.4.2	McLean's System Z and More Questions	166
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
6.2.1 Low-Water-Mark Policy	176
6.2.2 Ring Policy	177
6.2.3 Biba’s Model (Strict Integrity Policy)	177
6.3 Lipner’s Integrity Matrix Model	178
6.3.1 Lipner’s Use of the Bell-LaPadula Model	178
6.3.2 Lipner’s Full Model	181
6.3.3 Comparison with Biba	182
6.4 Clark-Wilson Integrity Model	183
6.4.1 The Model	184
6.4.2 Comparison with the Requirements	187
6.4.3 Comparison with Other Models	188
6.5 Trust Models	189
6.5.1 Policy-Based Trust Management	191
6.5.2 Reputation-Based Trust Management	194
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
7.3.1 Constraint-Based Model	204
7.3.2 State-Based Modes	210
7.4 Example: Availability and Network Flooding	215
7.4.1 Analysis	216
7.4.2 Intermediate Systems	216
7.4.3 TCP State and Memory Allocations	218
7.4.4 Other Flooding Attacks	221
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
8.1.1 Informal Description	228
8.1.2 Formal Model	230

8.1.3	Aggressive Chinese Wall Model	233
8.1.4	Bell-LaPadula and Chinese Wall Models	234
8.1.5	Clark-Wilson and Chinese Wall Models	236
8.2	Clinical Information Systems Security Policy	236
8.2.1	Bell-LaPadula and Clark-Wilson Models	239
8.3	Originator Controlled Access Control	239
8.3.1	Digital Rights Management	241
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
9.1.1	Composition of Bell-LaPadula Models	256
9.2	Deterministic Noninterference	259
9.2.1	Unwinding Theorem	263
9.2.2	Access Control Matrix Interpretation	266
9.2.3	Security Policies That Change over Time	268
9.2.4	Composition of Deterministic Noninterference-Secure Systems	270
9.3	Nondeducibility	271
9.3.1	Composition of Deducibly Secure Systems	273
9.4	Generalized Noninterference	274
9.4.1	Composition of Generalized Noninterference Systems	275
9.5	Restrictiveness	277
9.5.1	State Machine Model	277
9.5.2	Composition of Restrictive Systems	279
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
10.1.1	Overview of Cryptanalysis	290

10.2	Symmetric Cryptosystems	291
10.2.1	Transposition Ciphers	291
10.2.2	Substitution Ciphers	292
10.2.3	Data Encryption Standard	299
10.2.4	Other Modern Symmetric Ciphers	302
10.2.5	Advanced Encryption Standard	303
10.3	Public Key Cryptography	306
10.3.1	El Gamal	307
10.3.2	RSA	309
10.3.3	Elliptic Curve Ciphers	312
10.4	Cryptographic Checksums	315
10.4.1	HMAC	317
10.5	Digital Signatures	318
10.5.1	Symmetric Key Signatures	319
10.5.2	Public Key Signatures	319
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
11.2.1	Symmetric Cryptographic Key Exchange	333
11.2.2	Kerberos	337
11.2.3	Public Key Cryptographic Key Exchange and Authentication	338
11.3	Key Generation	341
11.4	Cryptographic Key Infrastructures	343
11.4.1	Merkle's Tree Authentication Scheme	344
11.4.2	Certificate Signature Chains	346
11.4.3	Public Key Infrastructures	350
11.5	Storing and Revoking Keys	353
11.5.1	Key Storage	353
11.5.2	Key Revocation	358
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
12.1.1 Precomputing the Possible Messages	367
12.1.2 Misordered Blocks	368
12.1.3 Statistical Regularities	368
12.1.4 Type Flaw Attacks	369
12.1.5 Summary	370
12.2 Stream and Block Ciphers	370
12.2.1 Stream Ciphers	371
12.2.2 Block Ciphers	374
12.3 Authenticated Encryption	377
12.3.1 Counter with CBC-MAC Mode	377
12.3.2 Galois Counter Mode	379
12.4 Networks and Cryptography	381
12.5 Example Protocols	384
12.5.1 Secure Electronic Mail: PEM and OpenPGP	384
12.5.2 Instant Messaging	389
12.5.3 Security at the Transport Layer: TLS and SSL	393
12.5.4 Security at the Network Layer: IPsec	402
12.5.5 Conclusion	410
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
13.3.1 Random Selection of Passwords	418
13.3.2 Pronounceable and Other Computer-Generated Passwords	420
13.3.3 User Selection of Passwords	421
13.3.4 Graphical Passwords	425
13.4 Attacking Passwords	426
13.4.1 Off-Line Dictionary Attacks	428
13.4.2 On-Line Dictionary Attacks	430
13.4.3 Password Strength	432

13.5	Password Aging	434
13.5.1	One-Time Passwords	436
13.6	Challenge-Response	438
13.6.1	Pass Algorithms	438
13.6.2	Hardware-Supported Challenge-Response Procedures	439
13.6.3	Challenge-Response and Dictionary Attacks	439
13.7	Biometrics	441
13.7.1	Fingerprints	442
13.7.2	Voices	443
13.7.3	Eyes	443
13.7.4	Faces	444
13.7.5	Keystrokes	444
13.7.6	Combinations	445
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
14.2.1	Principle of Least Privilege	457
14.2.2	Principle of Fail-Safe Defaults	458
14.2.3	Principle of Economy of Mechanism	459
14.2.4	Principle of Complete Mediation	460
14.2.5	Principle of Open Design	461
14.2.6	Principle of Separation of Privilege	463
14.2.7	Principle of Least Common Mechanism	463
14.2.8	Principle of Least Astonishment	464
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
15.5.1	Conflicts	479
15.5.2	The Meaning of the Identity	481
15.5.3	Trust	482
15.6	Identity on the Web	484
15.6.1	Host Identity	484
15.6.2	State and Cookies	488
15.7	Anonymity on the Web	490
15.7.1	Email Anonymizers	491
15.7.2	Onion Routing	495
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
16.1.1	Abbreviations of Access Control Lists	508
16.1.2	Creation and Maintenance of Access Control Lists	511
16.1.3	Revocation of Rights	514
16.1.4	Example: NTFS and Access Control Lists	515
16.2	Capabilities	518
16.2.1	Implementation of Capabilities	519
16.2.2	Copying and Amplifying Capabilities	520
16.2.3	Revocation of Rights	522
16.2.4	Limits of Capabilities	522
16.2.5	Comparison with Access Control Lists	523
16.2.6	Privileges	524
16.3	Locks and Keys	526
16.3.1	Type Checking	528
16.3.2	Sharing Secrets	529
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
17.1.1	Entropy-Based Analysis	540
17.1.2	Information Flow Models and Mechanisms	541

- 17.2 Nonlattice Information Flow Policies 542
 - 17.2.1 Confinement Flow Model 543
 - 17.2.2 Transitive Nonlattice Information Flow Policies 544
 - 17.2.3 Nontransitive Information Flow Policies 545
- 17.3 Static Mechanisms 548
 - 17.3.1 Declarations 549
 - 17.3.2 Program Statements 550
 - 17.3.3 Exceptions and Infinite Loops 557
 - 17.3.4 Concurrency 558
 - 17.3.5 Soundness 561
- 17.4 Dynamic Mechanisms 562
 - 17.4.1 Fenton’s Data Mark Machine 562
 - 17.4.2 Variable Classes 565
- 17.5 Integrity Mechanisms 566
- 17.6 Example Information Flow Controls 567
 - 17.6.1 Privacy and Android Cell Phones 568
 - 17.6.2 Firewalls 570
- 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
 - 18.2.1 Controlled Environment 582
 - 18.2.2 Program Modification 590
- 18.3 Covert Channels 594
 - 18.3.1 Detection of Covert Channels 596
 - 18.3.2 Analysis of Covert Channels 610
 - 18.3.3 Mitigation of Covert Channels 616
- 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
 - 19.1.1 The Need for Assurance 629

19.1.2	The Role of Requirements in Assurance	631
19.1.3	Assurance throughout the Life Cycle	632
19.2	Building Secure and Trusted Systems	634
19.2.1	Life Cycle	634
19.2.2	The Waterfall Life Cycle Model	639
19.2.3	Agile Software Development	641
19.2.4	Other Models of Software Development	644
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
20.1.1	Threats and Security Objectives	650
20.1.2	Architectural Considerations	651
20.1.3	Policy Definition and Requirements Specification	657
20.1.4	Justifying Requirements	660
20.2	Assurance during System and Software Design	662
20.2.1	Design Techniques That Support Assurance	662
20.2.2	Design Document Contents	665
20.2.3	Building Documentation and Specification	675
20.2.4	Justifying That Design Meets Requirements	677
20.3	Assurance in Implementation and Integration	685
20.3.1	Implementation Considerations That Support Assurance	685
20.3.2	Assurance through Implementation Management	686
20.3.3	Justifying That the Implementation Meets the Design	687
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
21.3.1	The Hierarchical Development Methodology	705
21.3.2	Enhanced HDM	710
21.3.3	The Gypsy Verification Environment	711

21.4	Current Verification Systems	713
21.4.1	The Prototype Verification System	713
21.4.2	The Symbolic Model Verifier	716
21.4.3	The Naval Research Laboratory Protocol Analyzer	720
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
22.1.1	Deciding to Evaluate	728
22.1.2	Historical Perspective of Evaluation Methodologies	729
22.2	TCSEC: 1983–1999	730
22.2.1	TCSEC Requirements	731
22.2.2	The TCSEC Evaluation Classes	733
22.2.3	The TCSEC Evaluation Process	734
22.2.4	Impacts	735
22.3	International Efforts and the ITSEC: 1991–2001	737
22.3.1	ITSEC Assurance Requirements	739
22.3.2	The ITSEC Evaluation Levels	740
22.3.3	The ITSEC Evaluation Process	741
22.3.4	Impacts	741
22.4	Commercial International Security Requirements: 1991	742
22.4.1	CISR Requirements	743
22.4.2	Impacts	743
22.5	Other Commercial Efforts: Early 1990s	744
22.6	The Federal Criteria: 1992	744
22.6.1	FC Requirements	745
22.6.2	Impacts	745
22.7	FIPS 140: 1994–Present	746
22.7.1	FIPS 140 Requirements	746
22.7.2	FIPS 140-2 Security Levels	747
22.7.3	Additional FIPS 140-2 Documentation	748
22.7.4	Impact	748
22.7.5	Future	749
22.8	The Common Criteria: 1998–Present	749
22.8.1	Overview of the Methodology	751
22.8.2	CC Requirements	756
22.8.3	CC Security Functional Requirements	756

22.8.4	Assurance Requirements	759
22.8.5	Evaluation Assurance Levels	759
22.8.6	Evaluation Process	761
22.8.7	Other International Organizations	762
22.8.8	Impacts	763
22.8.9	Future of the Common Criteria	764
22.9	SSE-CMM: 1997–Present	765
22.9.1	The SSE-CMM Model	765
22.9.2	Using the SSE-CMM	767
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
23.2.1	Rootkits	777
23.2.2	Propagating Trojan Horses	779
23.3	Computer Viruses	780
23.3.1	Infection Vectors	782
23.3.2	Concealment	785
23.3.3	Summary	790
23.4	Computer Worms	790
23.5	Bots and Botnets	793
23.6	Other Malware	796
23.6.1	Rabbits and Bacteria	796
23.6.2	Logic Bombs	797
23.6.3	Adware	797
23.6.4	Spyware	799
23.6.5	Ransomware	800
23.6.6	Phishing	802
23.7	Combinations	803
23.8	Theory of Computer Viruses	803
23.9	Defenses	808
23.9.1	Scanning Defenses	808
23.9.2	Data and Instructions	811
23.9.3	Containment	812
23.9.4	Specifications as Restrictions	817

23.9.5	Limiting Sharing	817
23.9.6	Statistical Analysis	819
23.9.7	The Notion of Trust	819
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
24.2.1	Goals	827
24.2.2	Layering of Tests	828
24.2.3	Methodology at Each Layer	829
24.2.4	Flaw Hypothesis Methodology	830
24.2.5	Versions	833
24.2.6	Example: Penetration of the Michigan Terminal System	837
24.2.7	Example: Compromise of a Burroughs System	839
24.2.8	Example: Penetration of a Corporate Computer System	840
24.2.9	Example: Penetrating a UNIX System	841
24.2.10	Example: Penetrating a Windows System	843
24.2.11	Debate	844
24.2.12	Conclusion	845
24.3	Vulnerability Classification	845
24.3.1	Two Security Flaws	846
24.4	Frameworks	849
24.4.1	The RISOS Study	849
24.4.2	Protection Analysis Model	851
24.4.3	The NRL Taxonomy	857
24.4.4	Aslam's Model	859
24.4.5	Comparison and Analysis	860
24.5	Standards	864
24.5.1	Common Vulnerabilities and Exposures (CVE)	864
24.5.2	Common Weaknesses and Exposures (CWE)	866
24.6	Gupta and Gligor's Theory of Penetration Analysis	868
24.6.1	The Flow-Based Model of Penetration Analysis	869
24.6.2	The Automated Penetration Analysis Tool	872
24.6.3	Discussion	873
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
25.2.1 Logger	881
25.2.2 Analyzer	883
25.2.3 Notifier	883
25.3 Designing an Auditing System	884
25.3.1 Implementation Considerations	886
25.3.2 Syntactic Issues	887
25.3.3 Log Sanitization	888
25.3.4 Application and System Logging	891
25.4 A Posteriori Design	893
25.4.1 Auditing to Detect Violations of a Known Policy	893
25.4.2 Auditing to Detect Known Violations of a Policy	895
25.5 Auditing Mechanisms	897
25.5.1 Secure Systems	897
25.5.2 Nonsecure Systems	899
25.6 Examples: Auditing File Systems	900
25.6.1 Audit Analysis of the NFS Version 2 Protocol	900
25.6.2 The Logging and Auditing File System (LAFS)	905
25.6.3 Comparison	907
25.6.4 Audit Browsing	908
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
26.3.1 Anomaly Modeling	920
26.3.2 Misuse Modeling	932
26.3.3 Specification Modeling	938
26.3.4 Summary	941
26.4 Architecture	942
26.4.1 Agent	943
26.4.2 Director	945
26.4.3 Notifier	946
26.5 Organization of Intrusion Detection Systems	948
26.5.1 Monitoring Network Traffic for Intrusions: NSM	948
26.5.2 Combining Host and Network Monitoring: DIDS	949
26.5.3 Autonomous Agents: AAFID	952

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
27.2.1	Attack Trees	961
27.2.2	The Requires/Provides Model	965
27.2.3	Attack Graphs	969
27.3	Intrusion Response	971
27.3.1	Incident Prevention	971
27.3.2	Intrusion Handling	975
27.4	Digital Forensics	987
27.4.1	Principles	987
27.4.2	Practice	990
27.4.3	Anti-Forensics	994
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
28.2.1	Data Classes	1007
28.2.2	User Classes	1008
28.2.3	Availability	1010
28.2.4	Consistency Check	1010
28.3	Network Organization	1011
28.3.1	Analysis of the Network Infrastructure	1013
28.3.2	In the DMZ	1017
28.3.3	In the Internal Network	1021
28.3.4	General Comment on Assurance	1025
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
29.2.1	The WWW Server System in the DMZ	1036
29.2.2	The Development System	1037
29.2.3	Comparison	1041
29.2.4	Conclusion	1041
29.3	Networks	1042
29.3.1	The WWW Server System in the DMZ	1042
29.3.2	The Development System	1045
29.3.3	Comparison	1047
29.4	Users	1048
29.4.1	The WWW Server System in the DMZ	1048
29.4.2	The Development System	1050
29.4.3	Comparison	1052
29.5	Authentication	1053
29.5.1	The WWW Server System in the DMZ	1053
29.5.2	Development Network System	1054
29.5.3	Comparison	1055
29.6	Processes	1055
29.6.1	The WWW Server System in the DMZ	1055
29.6.2	The Development System	1059
29.6.3	Comparison	1060
29.7	Files	1061
29.7.1	The WWW Server System in the DMZ	1061
29.7.2	The Development System	1063
29.7.3	Comparison	1065
29.8	Retrospective	1066
29.8.1	The WWW Server System in the DMZ	1066
29.8.2	The Development System	1067
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
30.2.1	Passwords	1074
30.2.2	The Login Procedure	1076
30.2.3	Leaving the System	1079
30.3	Files and Devices	1080
30.3.1	Files	1080
30.3.2	Devices	1084
30.4	Processes	1087
30.4.1	Copying and Moving Files	1087
30.4.2	Accidentally Overwriting Files	1088
30.4.3	Encryption, Cryptographic Keys, and Passwords	1089
30.4.4	Startup Settings	1090
30.4.5	Limiting Privileges	1091
30.4.6	Malicious Logic	1091
30.5	Electronic Communications	1092
30.5.1	Automated Electronic Mail Processing	1092
30.5.2	Failure to Check Certificates	1093
30.5.3	Sending Unexpected Content	1094
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
31.2.1	Requirements	1100
31.2.2	Threats	1102
31.3	Design	1104
31.3.1	Framework	1104
31.3.2	Access to Roles and Commands	1106
31.4	Refinement and Implementation	1111
31.4.1	First-Level Refinement	1111
31.4.2	Second-Level Refinement	1112
31.4.3	Functions	1114
31.4.4	Summary	1117
31.5	Common Security-Related Programming Problems	1117
31.5.1	Improper Choice of Initial Protection Domain	1118
31.5.2	Improper Isolation of Implementation Detail	1123

- 31.5.3 Improper Change 1125
- 31.5.4 Improper Naming 1129
- 31.5.5 Improper Deallocation or Deletion 1131
- 31.5.6 Improper Validation 1132
- 31.5.7 Improper Indivisibility 1138
- 31.5.8 Improper Choice of Operand or Operation 1139
- 31.5.9 Summary 1141
- 31.6 Testing, Maintenance, and Operation 1141
 - 31.6.1 Testing 1142
 - 31.6.2 Testing Composed Modules 1145
 - 31.6.3 Testing the Program 1145
- 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.3.1 Joint Entropy 1166
 - C.3.2 Conditional Entropy 1167
 - C.3.3 Perfect Secrecy 1168
- C.4 Exercises 1169

Appendix D Virtual Machines	1171
D.1 Virtual Machine Structure	1171
D.2 Virtual Machine Monitor	1171
D.2.1 Privilege and Virtual Machines	1172
D.2.2 Physical Resources and Virtual Machines	1175
D.2.3 Paging and Virtual Machines	1175
D.3 Exercises	1176
Appendix E Symbolic Logic	1179
E.1 Propositional Logic	1179
E.1.1 Natural Deduction in Propositional Logic	1180
E.1.2 Rules	1180
E.1.3 Derived Rules	1181
E.1.4 Well-Formed Formulas	1182
E.1.5 Truth Tables	1182
E.1.6 Mathematical Induction	1183
E.2 Predicate Logic	1184
E.2.1 Natural Deduction in Predicate Logic	1185
E.3 Temporal Logic Systems	1186
E.3.1 Syntax of CTL	1186
E.3.2 Semantics of CTL	1186
E.4 Exercises	1188
Appendix F The Encryption Standards	1191
F.1 Data Encryption Standard	1191
F.1.1 Main DES Algorithm	1191
F.1.2 Round Key Generation	1195
F.2 Advanced Encryption Standard	1196
F.2.1 Background	1196
F.2.2 AES Encryption	1197
F.2.3 Encryption	1199
F.2.4 Round Key Generation	1201
F.2.5 Equivalent Inverse Cipher Implementation	1203
F.3 Exercises	1205
Appendix G Example Academic Security Policy	1207
G.1 Acceptable Use Policy	1207
G.1.1 Introduction	1208
G.1.2 Rights and Responsibilities	1208
G.1.3 Privacy	1208

G.1.4	Enforcement of Laws and University Policies	1209
G.1.5	Unacceptable Conduct	1209
G.1.6	Further Information	1212
G.2	University of California Electronic Communications Policy	1212
G.2.1	Introduction	1212
G.2.2	General Provisions	1213
G.2.3	Allowable Use	1216
G.2.4	Privacy and Confidentiality	1220
G.2.5	Security	1225
G.2.6	Retention and Disposition	1227
G.2.7	Appendix A: Definitions	1227
G.2.8	Appendix B: References	1230
G.2.9	Appendix C: Policies Relating to Access Without Consent	1232
G.3	User Advisories	1234
G.3.1	Introduction	1234
G.3.2	User Responsibilities	1234
G.3.3	Privacy Expectations	1235
G.3.4	Privacy Protections	1236
G.3.5	Privacy Limits	1237
G.3.6	Security Considerations	1239
G.4	Electronic Communications—Allowable Use	1241
G.4.1	Purpose	1241
G.4.2	Definitions	1242
G.4.3	Policy	1242
G.4.4	Allowable Users	1242
G.4.5	Allowable Uses	1243
G.4.6	Restrictions on Use	1245
G.4.7	References and Related Policies	1246
	Appendix H Programming Rules	1247
H.1	Implementation Rules	1247
H.2	Management Rules	1249
	References	1251
	Index	1341