1. An Overview of Computer Security 17
1.1. The Basic Components 17
1.1.1. Confidentiality 18
1.1.2. Integrity 19
1.1.3. Availability 20
1.2. Threats 20
1.3. Policy and Mechanism 23
1.3.1. Goals of Security 24
1.4. Assumptions and Trust 25
1.5. Assurance 26
1.5.1. Specification 27
1.5.2. Design 28
1.5.3. Implementation 28
1.6. Operational Issues 30
1.6.1. Cost-Benefit Analysis 30
1.6.2. Risk Analysis 31
1.6.3. Laws and Customs 32
1.7. Human Issues 33
1.7.1. Organizational Problems 34
1.7.2. People Problems 35
1.8. Tying It All Together 36
1.9. Summary 37
1.10. Further Reading 38
1.11. Exercises 38
2. Access Control Matrix 43
2.1. Protection State 43
2.2. Access Control Matrix Model 44
2.3. Protection State Transitions 47
2.3.1. Conditional Commands 49
2.4. Summary 50
2.5. Further Reading 51
2.6. Exercises 51
3. Foundational Results 53
3.1. The General Question 53
3.2. Basic Results 54
3.3. Summary 59
3.4. Exercises 60
4. Security Policies 61
4.1. Security Policies 61
4.2. Types of Security Policies 65

4.3. The Role of Trust 67
4.4. Types of Access Control 69
4.5. Example: Academic Computer Security Policy 70
4.5.1. General University Policy 71
4.5.2. Electronic Mail Policy 71
4.5.2.1. The Electronic Mail Policy Summary *72*
4.5.2.2. The Full Policy *72*
4.5.2.3. Implementation at UC Davis *73*
4.6. Summary 74
4.7. Further Reading 74
4.8. Exercises 75
5. Confidentiality Policies 77
5.1. Goals of Confidentiality Policies 77
5.2. The Bell-LaPadula Model 78
5.2.1. Informal Description 78
5.2.2. Example: The Data General B2 UNIX System 82
5.2.2.1. Assigning MAC Labels *82*
5.2.2.2. Using MAC Labels *85*
5.3. Summary 86
5.4. Further Reading 86
5.5. Exercises 87
6. Integrity Policies 89
6.1. Goals 89
6.2. Biba Integrity Model 91
6.3. Clark-Wilson Integrity Model 92
6.3.1. The Model 93
6.3.2. Comparison with the Requirements 95
6.3.3. Comparison with Other Models 96
6.4. Summary 97
6.5. Exercises 98
7. Hybrid Policies 99
7.1. Chinese Wall Model 99
7.1.1. Bell-LaPadula and Chinese Wall Models 102
7.1.2. Clark-Wilson and Chinese Wall Models 103
7.2. Clinical Information Systems Security Policy 104
7.2.1. Bell-LaPadula and Clark-Wilson Models 106
7.3. Originator Controlled Access Control 107
7.4. Role-Based Access Control 109
7.5. Summary 111
7.6. Further Reading 111
7.7. Exercises 111

8. Basic Cryptography 113
8.1. What Is Cryptography? 113
8.2. Classical Cryptosystems 114
8.2.1. Transposition Ciphers 115
8.2.2. Substitution Ciphers 116
8.2.2.1. Vigenère Cipher 117
8.2.2.2. One-Time Pad 123
8.2.3. Data Encryption Standard 124
8.2.4. Other Classical Ciphers 128
8.3. Public Key Cryptography 129
8.3.1. RSA 129
8.4. Cryptographic Checksums 132
8.4.1. HMAC 134
8.5. Summary 135
8.6. Further Reading 135
8.7. Exercises 136
9. Key Management 139
9.1. Session and Interchange Keys 140
9.2. Key Exchange 140
9.2.1. Classical Cryptographic Key Exchange and Authentication . 141
9.2.2. Kerberos 144
9.2.3. Public Key Cryptographic Key Exchange and Authentication 145
9.3. Cryptographic Key Infrastructures 146
9.3.1. Certificate Signature Chains 147
9.3.1.1. X.509: Certification Signature Chains 148
9.3.1.2. PGP Certificate Signature Chains 150
9.3.2. Summary 152
9.4. Storing and Revoking Keys 152
9.4.1. Key Storage 152
9.4.2. Key Revocation 153
9.5. Digital Signatures 153
9.5.1. Classical Signatures 154
9.5.2. Public Key Signatures 155
9.6. Summary 156
9.7. Further Reading 157
9.8. Exercises 158
10. Cipher Techniques 161
10.1. Problems 161
10.1.1. Precomputing the Possible Messages 161
10.1.2. Misordered Blocks 162
10.1.3. Statistical Regularities 162

10.1.4. Summary 163
10.2. Stream and Block Ciphers 163
10.2.1. Stream Ciphers 163
10.2.1.1. Synchronous Stream Ciphers *164*
10.2.1.2. Self-Synchronous Stream Ciphers *166*
10.2.2. Block Ciphers 167
10.2.2.1. Multiple Encryption *168*
10.3. Networks and Cryptography 169
10.4. Example Protocols 172
10.4.1. Secure Electronic Mail: PEM 172
10.4.1.1. Design Principles *173*
10.4.1.2. Basic Design *174*
10.4.1.3. Other Considerations *175*
10.4.1.4. Conclusion *176*
10.4.2. Security at the Network Layer: IPsec 177
10.4.2.1. IPsec Architecture *178*
10.4.2.2. Authentication Header Protocol *181*
10.4.2.3. Encapsulating Security Payload Protocol *182*
10.4.3. Conclusion 183
10.5. Summary 184
10.6. Further Reading 185
10.7. Exercises 185
11. Authentication 187
11.1. Authentication Basics 187
11.2. Passwords 188
11.2.1. Attacking a Password System 190
11.2.2. Countering Password Guessing 191
11.2.2.1. Random Selection of Passwords *192*
11.2.2.2. Pronounceable and Other Computer-Generated Passwords *193*
11.2.2.3. User Selection of Passwords *194*
11.2.2.4. Reusable Passwords and Dictionary Attacks . . . *198*
11.2.2.5. Guessing Through Authentication Functions . . . *199*
11.2.3. Password Aging 200
11.3. Challenge-Response 202
11.3.1. Pass Algorithms 202
11.3.2. One-Time Passwords 203
11.3.3. Hardware-Supported Challenge-Response Procedures 204
11.3.4. Challenge-Response and Dictionary Attacks 205
11.4. Biometrics 206
11.4.1. Fingerprints 206

11.4.2. Voices 207
11.4.3. Eyes 207
11.4.4. Faces 207
11.4.5. Keystrokes 208
11.4.6. Combinations 208
11.4.7. Caution 208
11.5. Multiple Methods 209
11.6. Summary 211
11.7. Exercises 212
12. Design Principles 217
12.1. Overview 217
12.2. Design Principles 219
12.2.1. Principle of Least Privilege 219
12.2.2. Principle of Fail-Safe Defaults 220
12.2.3. Principle of Economy of Mechanism 220
12.2.4. Principle of Complete Mediation 221
12.2.5. Principle of Open Design 222
12.2.6. Principle of Separation of Privilege 223
12.2.7. Principle of Least Common Mechanism 224
12.2.8. Principle of Psychological Acceptability 224
12.3. Summary 225
12.4. Exercises 226
13. Representing Identity 229
13.1. What Is Identity? 229
13.2. Files and Objects 230
13.3. Users 231
13.4. Groups and Roles 232
13.5. Naming and Certificates 233
13.5.1. The Meaning of the Identity 236
13.5.2. Trust 238
13.6. Identity on the Web 239
13.6.1. Host Identity 239
13.6.1.1. Static and Dynamic Identifiers 240
13.6.1.2. Security Issues with the Domain Name Service . 242
13.6.2. State and Cookies 243
13.6.3. Anonymity on the Web 244
13.6.3.1. Anonymity for Better or Worse 248
13.7. Summary 251
13.8. Further Reading 251
13.9. Exercises 252
14. Access Control Mechanisms 255

14.1. Access Control Lists. 255
14.1.1. Abbreviations of Access Control Lists. 256
14.1.2. Creation and Maintenance of Access Control Lists 258
14.1.2.1. Which Subjects Can Modify an Object's ACL? . 259
14.1.2.2. Do the ACLs Apply to a Privileged User? 259
14.1.2.3. Does the ACL Support Groups and Wildcards? 260
14.1.2.4. Conflicts 260
14.1.2.5. ACLs and Default Permissions. 261
14.1.3. Revocation of Rights 261
14.1.4. Example: Windows NT Access Control Lists 262
14.2. Capabilities. 264
14.2.1. Implementation of Capabilities 265
14.2.2. Copying and Amplifying Capabilities 266
14.2.3. Revocation of Rights 267
14.2.4. Limits of Capabilities 268
14.2.5. Comparison with Access Control Lists 269
14.3. Locks and Keys 270
14.3.1. Type Checking 271
14.4. Ring-Based Access Control 273
14.5. Propagated Access Control Lists 275
14.6. Summary 276
14.7. Exercises. 277
15. Information Flow 279
15.1. Basics and Background 279
15.1.1. Information Flow Models and Mechanisms. 281
15.2. Compiler-Based Mechanisms 281
15.2.1. Declarations 282
15.2.2. Program Statements 284
15.2.2.1. Assignment Statements 284
15.2.2.2. Compound Statements 285
15.2.2.3. Conditional Statements. 285
15.2.2.4. Iterative Statements 286
15.2.2.5. Goto Statements 287
15.2.2.6. Procedure Calls 290
15.2.3. Exceptions and Infinite Loops 290
15.2.4. Concurrency 292
15.2.5. Soundness. 295
15.3. Execution-Based Mechanisms 295
15.3.1. Fenton's Data Mark Machine. 296
15.3.2. Variable Classes 298
15.4. Example Information Flow Controls 300

15.4.1. Security Pipeline Interface 300
15.4.2. Secure Network Server Mail Guard 300
15.5. Summary 302
15.6. Exercises 303
16. Confinement Problem 305
16.1. The Confinement Problem 305
16.2. Isolation 308
16.2.1. Virtual Machines 308
16.2.2. Sandboxes 310
16.3. Covert Channels 312
16.3.1. Detection of Covert Channels 314
16.3.2. Mitigation of Covert Channels 322
16.4. Summary 324
16.5. Exercises 325
17. Introduction to Assurance. 327
17.1. Assurance and Trust 327
17.1.1. The Need for Assurance 329
17.1.2. The Role of Requirements in Assurance 331
17.1.3. Assurance Throughout the Life Cycle 332
17.2. Building Secure and Trusted Systems. 334
17.2.1. Life Cycle 334
17.2.1.1. Conception 335
17.2.1.2. Manufacture 336
17.2.1.3. Deployment 337
17.2.1.4. Fielded Product Life 338
17.2.2. The Waterfall Life Cycle Model 338
17.2.2.1. Requirements Definition and Analysis 338
17.2.2.2. System and Software Design 339
17.2.2.3. Implementation and Unit Testing 339
17.2.2.4. Integration and System Testing 340
17.2.2.5. Operation and Maintenance 340
17.2.2.6. Discussion 340
17.2.3. Other Models of Software Development 341
17.2.3.1. Exploratory Programming 341
17.2.3.2. Prototyping 341
17.2.3.3. Formal Transformation 341
17.2.3.4. System Assembly from Reusable Components . . 342
17.2.3.5. Extreme Programming 342
17.3. Building Security In or Adding Security Later 342
17.4. Summary 346
17.5. Further Reading. 346

17.6. Exercises 347
18. Evaluating Systems 349
18.1. Goals of Formal Evaluation 349
18.1.1. Deciding to Evaluate 350
18.1.2. Historical Perspective of Evaluation Methodologies 351
18.2. TCSEC: 1983–1999 352
18.2.1. TCSEC Requirements 353
18.2.1.1. TCSEC Functional Requirements 353
18.2.1.2. TCSEC Assurance Requirements 354
18.2.2. The TCSEC Evaluation Classes 355
18.2.3. The TCSEC Evaluation Process 356
18.2.4. Impacts 356
18.2.4.1. Scope Limitations 357
18.2.4.2. Process Limitations 357
18.2.4.3. Contributions 358
18.3. FIPS 140: 1994–Present 359
18.3.1. FIPS 140 Requirements 359
18.3.2. FIPS 140-2 Security Levels 360
18.3.3. Impact 360
18.4. The Common Criteria: 1998–Present 361
18.4.1. Overview of the Methodology 362
18.4.2. CC Requirements 366
18.4.3. CC Security Functional Requirements 367
18.4.4. Assurance Requirements 369
18.4.5. Evaluation Assurance Levels 369
18.4.6. Evaluation Process 371
18.4.7. Impacts 372
18.4.8. Future of the Common Criteria 372
18.4.8.1. Interpretations 372
18.4.8.2. Assurance Class AMA and Family ALC_FLR . . 373
18.4.8.3. Products Versus Systems 373
18.4.8.4. Protection Profiles and Security Targets 373
18.4.8.5. Assurance Class AVA 374
18.4.8.6. EAL5 374
18.5. SSE-CMM: 1997–Present 374
18.5.1. The SSE-CMM Model 375
18.5.2. Using the SSE-CMM 376
18.6. Summary 377
18.7. Further Reading 378
18.8. Exercises 379
19. Malicious Logic 381

19.1. Introduction 381
19.2. Trojan Horses 382
19.3. Computer Viruses 383
19.3.1. Boot Sector Infectors. 385
19.3.2. Executable Infectors 386
19.3.3. Multipartite Viruses 387
19.3.4. TSR Viruses 388
19.3.5. Stealth Viruses 388
19.3.6. Encrypted Viruses 388
19.3.7. Polymorphic Viruses 389
19.3.8. Macro Viruses 390
19.4. Computer Worms 391
19.5. Other Forms of Malicious Logic. 392
19.5.1. Rabbits and Bacteria 392
19.5.2. Logic Bombs 393
19.6. Defenses 394
19.6.1. Malicious Logic Acting as Both Data and Instructions 394
19.6.2. Malicious Logic Assuming the Identity of a User 395
19.6.2.1. Information Flow Metrics 395
19.6.2.2. Reducing the Rights. 396
19.6.2.3. Sandboxing 399
19.6.3. Malicious Logic Crossing Protection Domain Boundaries by Sharing 399
19.6.4. Malicious Logic Altering Files 400
19.6.5. Malicious Logic Performing Actions Beyond Specification 401
19.6.5.1. Proof-Carrying Code 402
19.6.6. Malicious Logic Altering Statistical Characteristics. 402
19.6.7. The Notion of Trust. 403
19.7. Summary 404
19.8. Further Reading. 404
19.9. Exercises 405
20. Vulnerability Analysis 407
20.1. Introduction 407
20.2. Penetration Studies 409
20.2.1. Goals 409
20.2.2. Layering of Tests. 410
20.2.3. Methodology at Each Layer 411
20.2.4. Flaw Hypothesis Methodology 411
20.2.4.1. Information Gathering and Flaw Hypothesis . . . 412
20.2.4.2. Flaw Testing 413
20.2.4.3. Flaw Generalization 413

20.2.4.4. Flaw Elimination 414
20.2.5. Example: Penetration of the Michigan Terminal System . . 414
20.2.6. Example: Compromise of a Burroughs System 416
20.2.7. Example: Penetration of a Corporate Computer System . . . 417
20.2.8. Example: Penetrating a UNIX System 418
20.2.9. Example: Penetrating a Windows NT System 420
20.2.10. Debate 421
20.2.11. Conclusion 422
20.3. Vulnerability Classification 422
20.3.1. Two Security Flaws 423
20.4. Frameworks 424
20.4.1. The RISOS Study 424
20.4.1.1. The Flaw Classes 426
20.4.1.2. Legacy 427
20.4.2. Protection Analysis Model 427
20.4.2.1. The Flaw Classes 428
20.4.2.2. Legacy 430
20.4.3. The NRL Taxonomy 430
20.4.3.1. The Flaw Classes 430
20.4.3.2. Legacy 432
20.4.4. Aslam's Model 432
20.4.4.1. The Flaw Classes 433
20.4.4.2. Legacy 433
20.4.5. Comparison and Analysis 433
20.4.5.1. The xterm Log File Flaw 434
20.4.5.2. The fingerd Buffer Overflow Flaw 436
20.4.5.3. Summary 437
20.5. Further Reading 438
20.6. Exercises 439
21. Auditing 441
21.1. Definitions 441
21.2. Anatomy of an Auditing System 442
21.2.1. Logger 442
21.2.2. Analyzer 444
21.2.3. Notifier 445
21.3. Designing an Auditing System 445
21.3.1. Implementation Considerations 447
21.3.2. Syntactic Issues 447
21.3.3. Log Sanitization 449
21.3.4. Application and System Logging 451
21.4. A Posteriori Design 452

21.4.1. Auditing to Detect Violations of a Known Policy 453
21.4.1.1. State-Based Auditing 453
21.4.1.2. Transition-Based Auditing 454
21.4.2. Auditing to Detect Known Violations of a Policy 455
21.5. Auditing Mechanisms 456
21.5.1. Secure Systems 456
21.5.2. Nonsecure Systems 458
21.6. Examples: Auditing File Systems 459
21.6.1. Audit Analysis of the NFS Version 2 Protocol 459
21.6.2. The Logging and Auditing File System (LAFS) 464
21.6.3. Comparison 465
21.7. Audit Browsing 466
21.8. Summary 469
21.9. Further Reading 469
21.10. Exercises 470
22. Intrusion Detection 473
22.1. Principles 473
22.2. Basic Intrusion Detection 474
22.3. Models 476
22.3.1. Anomaly Modeling 477
22.3.2. Misuse Modeling 479
22.3.3. Specification Modeling 481
22.3.4. Summary 482
22.4. Architecture 483
22.4.1. Agent 483
22.4.1.1. Host-Based Information Gathering 484
22.4.1.2. Network-Based Information Gathering 485
22.4.1.3. Combining Sources 485
22.4.2. Director 487
22.4.3. Notifier 488
22.5. Organization of Intrusion Detection Systems 489
22.5.1. Monitoring Network Traffic for Intrusions: NSM 490
22.5.2. Combining Host and Network Monitoring: DIDS 491
22.5.3. Autonomous Agents: AAFID 493
22.6. Intrusion Response 495
22.6.1. Incident Prevention 495
22.6.2. Intrusion Handling 496
22.6.2.1. Containment Phase 496
22.6.2.2. Eradication Phase 498
22.6.2.3. Follow-Up Phase 501
22.7. Exercises 504

23. Network Security 507
23.1. Introduction 507
23.2. Policy Development 508
23.2.1. Data Classes 509
23.2.2. User Classes 510
23.2.3. Availability 512
23.2.4. Consistency Check 512
23.3. Network Organization 513
23.3.1. Firewalls and Proxies 514
23.3.2. Analysis of the Network Infrastructure 516
23.3.2.1. Outer Firewall Configuration 517
23.3.2.2. Inner Firewall Configuration 519
23.3.3. In the DMZ 520
23.3.3.1. DMZ Mail Server 520
23.3.3.2. DMZ WWW Server 521
23.3.3.3. DMZ DNS Server 523
23.3.3.4. DMZ Log Server 523
23.3.3.5. Summary 524
23.3.4. In the Internal Network 524
23.3.5. General Comment on Assurance 526
23.4. Availability and Network Flooding 527
23.4.1. Intermediate Hosts 527
23.4.2. TCP State and Memory Allocations 528
23.5. Anticipating Attacks 530
23.6. Summary 532
23.7. Exercises 533
24. System Security 539
24.1. Introduction 539
24.2. Policy 540
24.2.1. The Web Server System in the DMZ 540
24.2.2. The Development System 541
24.2.3. Comparison 544
24.2.4. Conclusion 545
24.3. Networks 545
24.3.1. The Web Server System in the DMZ 546
24.3.2. The Development System 548
24.3.3. Comparison 550
24.4. Users 551
24.4.1. The Web Server System in the DMZ 551
24.4.2. The Development System 553
24.4.3. Comparison 556

24.5. Authentication 556
24.5.1. The Web Server System in the DMZ 557
24.5.2. Development Network System 557
24.5.3. Comparison 559
24.6. Processes 559
24.6.1. The Web Server System in the DMZ 559
24.6.2. The Development System 563
24.6.3. Comparison 564
24.7. Files 565
24.7.1. The Web Server System in the DMZ 565
24.7.2. The Development System 567
24.7.3. Comparison 569
24.8. Retrospective 571
24.8.1. The Web Server System in the DMZ 571
24.8.2. The Development System 572
24.9. Summary 572
24.10. Further Reading 573
24.11. Exercises 573
25. User Security 577
25.1. Policy 577
25.2. Access 578
25.2.1. Passwords 578
25.2.2. The Login Procedure 580
25.2.2.1. Trusted Hosts 582
25.2.3. Leaving the System 582
25.3. Files and Devices 584
25.3.1. Files 584
25.3.1.1. File Permissions on Creation 585
25.3.1.2. Group Access 586
25.3.1.3. File Deletion 587
25.3.2. Devices 589
25.3.2.1. Writable Devices 589
25.3.2.2. Smart Terminals 589
25.3.2.3. Monitors and Window Systems 591
25.4. Processes 592
25.4.1. Copying and Moving Files 592
25.4.2. Accidentally Overwriting Files 593
25.4.3. Encryption, Cryptographic Keys, and Passwords 593
25.4.4. Start-up Settings 595
25.4.5. Limiting Privileges 595
25.4.6. Malicious Logic 596

25.5. Electronic Communications 597
25.5.1. Automated Electronic Mail Processing 597
25.5.2. Failure to Check Certificates 597
25.5.3. Sending Unexpected Content 598
25.6. Summary 598
25.7. Further Reading 599
25.8. Exercises. 600
26. . . . . Program Security601
26.1. Introduction 601
26.2. Requirements and Policy 602
26.2.1. Requirements 602
26.2.2. Threats 603
26.2.2.1. Group 1: Unauthorized Users Accessing Role Accounts. 603
26.2.2.2. Group 2: Authorized Users Accessing Role Accounts 604
26.2.2.3. Summary. 605
26.3. Design. 605
26.3.1. Framework 606
26.3.1.1. User Interface. 606
26.3.1.2. High-Level Design 606
26.3.2. Access to Roles and Commands 607
26.3.2.1. Interface 608
26.3.2.2. Internals 608
26.3.2.3. Storage of the Access Control Data 609
26.4. Refinement and Implementation 612
26.4.1. First-Level Refinement. 612
26.4.2. Second-Level Refinement 613
26.4.3. Functions 616
26.4.3.1. Obtaining Location. 616
26.4.3.2. The Access Control Record 617
26.4.3.3. Error Handling in the Reading and Matching Routines 618
26.4.4. Summary 619
26.5. Common Security-Related Programming Problems 619
26.5.1. Improper Choice of Initial Protection Domain. 620
26.5.1.1. Process Privileges 620
26.5.1.2. Access Control File Permissions 622
26.5.1.3. Memory Protection. 623
26.5.1.4. Trust in the System 624
26.5.2. Improper Isolation of Implementation Detail. 625

26.5.2.1. Resource Exhaustion and User Identifiers 625
26.5.2.2. Validating the Access Control Entries 626
26.5.2.3. Restricting the Protection Domain of the Role Process 626
26.5.3. Improper Change 627
26.5.3.1. Memory 627
26.5.3.2. Changes in File Contents 630
26.5.3.3. Race Conditions in File Accesses 630
26.5.4. Improper Naming 631
26.5.5. Improper Deallocation or Deletion 633
26.5.6. Improper Validation 634
26.5.6.1. Bounds Checking 634
26.5.6.2. Type Checking 635
26.5.6.3. Error Checking 636
26.5.6.4. Checking for Valid, not Invalid, Data 636
26.5.6.5. Checking Input 637
26.5.6.6. Designing for Validation 639
26.5.7. Improper Indivisibility 639
26.5.8. Improper Sequencing 640
26.5.9. Improper Choice of Operand or Operation 641
26.5.10. Summary 643
26.6. Testing, Maintenance, and Operation 645
26.6.1. Testing 646
26.6.1.1. Testing the Module 647
26.6.2. Testing Composed Modules 648
26.6.3. Testing the Program 649
26.7. Distribution 649
26.8. Further Reading 651
26.9. Exercises 652
27. Lattices 655
27.1. Basics 655
27.2. Lattices 656
27.3. Exercises 657
28. The Extended Euclidean Algorithm 659
28.1. The Euclidean Algorithm 659
28.2. The Extended Euclidean Algorithm 660
28.3. Solving ax mod n = 1 662
28.4. Solving ax mod n = b 662
28.5. Exercises 663
29. Virtual Machines 665

29.1. Virtual Machine Structure 665
29.2. Virtual Machine Monitor 666
29.2.1. Privilege and Virtual Machines 667
29.2.2. Physical Resources and Virtual Machines 668
29.2.3. Paging and Virtual Machines 669
29.3. Exercises. 670
30. Bibliography 671