

# Contents

Contributors xxvii  
About the Editor xxxi  
Foreword xxxiii  
Preface xxxv  
Acknowledgments xli

## Part I Overview of System and Network Security: A Comprehensive Introduction 1

### 1. Information Security in the Modern Enterprise 3

*James Pooley*

1. Introduction 3
2. Challenges Facing Information Security 4
3. Assessment and Planning 5
4. Policies and Procedures 8
5. Training 9
6. Summary 10
- Chapter Review Questions/Exercises 10
- Exercise 11

### 2. Building a Secure Organization 13

*John R. Mallery*

1. Obstacles to Security 13
2. Computers Are Powerful and Complex 13
3. Current Trend Is to Share, Not Protect 14
4. Security Is Not About Hardware and Software 16
5. Ten Steps to Building a Secure Organization 18
6. Preparing for the Building of Security Control Assessments 31
7. Summary 31
- Chapter Review Questions/Exercises 33
- Exercise 33

### 3. A Cryptography Primer 35

*Scott R. Ellis*

1. What Is Cryptography? What Is Encryption? 36
2. Famous Cryptographic Devices 36
3. Ciphers 37
4. Modern Cryptography 44
5. The Computer Age 49
6. How Advanced Encryption Standard Works 52
7. Selecting Cryptography: the Process 55
8. Summary 56
- Chapter Review Questions/Exercises 57
- Exercise 57

### 4. Verifying User and Host Identity 59

*Keith Lewis*

1. Introduction: Verifying the User 59
2. Identity Access Management: Authentication and Authorization 59
3. Synthetic or Real User Logging 61
4. Verifying a User in Cloud Environments 62
5. Verifying Hosts 63
6. Verifying Host Domain Name System and Internet Protocol Information 63
7. Summary 64
8. Chapter Review Questions/Exercises 64
- Exercise 65
- References 65

### 5. Detecting System Intrusions 67

*Scott R. Ellis*

1. Introduction 67
2. Developing Threat Models 69
3. Securing Communications 70
4. Network Security Monitoring and Intrusion Detection Systems 74
5. Installing Security Onion to a Bare-Metal Server 83

- 6. Putting It All Together 86
  - 7. Securing Your Installation 87
  - 8. Managing an Intrusion Detection System in a Network Security Monitoring Framework 87
  - 9. Setting the Stage 93
  - 10. Alerts and Events 93
  - 11. Sguil: Tuning Graphics Processing Unit Rules, Alerts, and Responses 95
  - 12. Developing Process 99
  - 13. Understanding, Exploring, and Managing Alerts 100
  - 14. Summary 106
  - Chapter Review Questions/Exercises 107
  - Exercise 107
- 6. Intrusion Detection in Contemporary Environments 109**
- Tarfa Hamed, Rozita Dara, Stefan C. Kremer*
- 1. Introduction 109
  - 2. Mobile Operating Systems 110
  - 3. Mobile Device Malware Risks 111
  - 4. Cloud Computing Models 112
  - 5. Cloud Computing Attack Risks 112
  - 6. Source of Attacks on Mobile Devices 113
  - 7. Source or Origin of Intrusions in Cloud Computing 113
  - 8. Classes of Mobile Malware 114
  - 9. Types of Cloud Computing Attacks 114
  - 10. Malware Techniques in Android 115
  - 11. Cloud Computing Intrusions Techniques 117
  - 12. Examples of Smartphone Malware 118
  - 13. Examples of Cloud Attacks 119
  - 14. Types of Intrusion Detection Systems for Mobile Devices 121
  - 15. Types of Intrusion Detection Systems for Cloud Computing 123
  - 16. Intrusion Detection System Performance Metrics 126
  - 17. Summary 127
  - Chapter Review Questions/Exercises 128
  - Exercise 128
  - References 128
- 7. Preventing System Intrusions 131**
- Michael A. West*
- 1. So, What Is an Intrusion? 132
  - 2. Sobering Numbers 133
  - 3. Know Your Enemy: Hackers Versus Crackers 133
  - 4. Motives 134
  - 5. The Crackers' Tools of the Trade 134
  - 6. Bots 136
  - 7. Symptoms of Intrusions 136
  - 8. What Can You Do? 137
  - 9. Security Policies 139
  - 10. Risk Analysis 140
  - 11. Tools of Your Trade 141
  - 12. Controlling User Access 143
  - 13. Intrusion Prevention Capabilities 145
  - 14. Summary 145
  - Chapter Review Questions/Exercises 146
  - Exercise 146
- 8. Guarding Against Network Intrusions 149**
- Thomas M. Chen*
- 1. Introduction 149
  - 2. Traditional Reconnaissance and Attacks 149
  - 3. Malicious Software 152
  - 4. Defense in Depth 154
  - 5. Preventive Measures 155
  - 6. Intrusion Monitoring and Detection 159
  - 7. Reactive Measures 160
  - 8. Network-Based Intrusion Protection 161
  - 9. Summary 162
  - Chapter Review Questions/Exercises 162
  - Exercise 163
- 9. Fault Tolerance and Resilience in Cloud Computing Environments 165**
- Ravi Jhawar, Vincenzo Piuri*
- 1. Introduction 165
  - 2. Cloud Computing Fault Model 166
  - 3. Basic Concepts of Fault Tolerance 168
  - 4. Different Levels of Fault Tolerance in Cloud Computing 170
  - 5. Fault Tolerance Against Crash Failures in Cloud Computing 171
  - 6. Fault Tolerance Against Byzantine Failures in Cloud Computing 173
  - 7. Fault Tolerance as a Service in Cloud Computing 175
  - 8. Summary 179
  - Chapter Review Questions/Exercises 180
  - Exercise 180
  - Acknowledgments 180
  - References 180

**10. Securing Web Applications, Services, and Servers 183***Gerald Beuchelt*

1. Setting the Stage 183
  2. Basic Security for HTTP Applications and Services 184
  3. Basic Security for SOAP Services 187
  4. Identity Management and Web Services 189
  5. Authorization Patterns 195
  6. Security Considerations 196
  7. Challenges 201
  8. Summary 202
- Chapter Review Questions/Exercises 202  
Exercise 203  
Resources 203

**11. UNIX and Linux Security 205***Gerald Beuchelt*

1. Introduction 205
  2. UNIX and Security 205
  3. Basic UNIX Security Overview 206
  4. Achieving UNIX Security 209
  5. Protecting User Accounts and Strengthening Authentication 211
  6. Limiting Superuser Privileges 215
  7. Securing Local and Network File Systems 217
  8. Network Configuration 219
  9. Improving the Security of Linux and UNIX Systems 221
  10. Additional Resources 222
  11. Summary 223
- Chapter Review Questions/Exercises 223  
Exercise 224

**12. Eliminating the Security Weakness of Linux and UNIX Operating Systems 225***Mario Santana*

1. Introduction to Linux and UNIX 225
  2. Hardening Linux and UNIX 229
  3. Proactive Defense for Linux and UNIX 236
  4. Summary 237
- Chapter Review Questions/Exercises 238  
Exercise 238

**13. Internet Security 239***Jesse Walker*

1. Internet Protocol Architecture 239
  2. An Internet Threat Model 246
  3. Defending Against Attacks on the Internet 251
  4. Internet Security Checklist 262
  5. Summary 262
- Chapter Review Questions/Exercises 263  
Exercise 263

**14. The Botnet Problem 265***Nailah Mims*

1. Introduction 265
  2. What Is a Botnet? 265
  3. Building a Botnet 265
  4. The Problem With Botnets 268
  5. Botnet Case Studies and Known Botnets 270
  6. Summary 272
- Chapter Review Questions/Exercises 272  
Exercise 273  
References 274

**15. Intranet Security 275***Bill Mansoor*

1. Smartphones and Tablets in the Intranet 277
2. Security Considerations 281
3. Plugging the Gaps: Network Access Control and Access Control 283
4. Measuring Risk: Audits 284
5. Guardian at the Gate: Authentication and Encryption 286
6. Wireless Network Security 286
7. Shielding the Wire: Network Protection 287
8. Weakest Link in Security: User Training 289
9. Documenting the Network: Change Management 289
10. Rehearse the Inevitable: Disaster Recovery 290
11. Controlling Hazards: Physical and Environmental Protection 292
12. Know Your Users: Personnel Security 293

13. Protecting Data Flow: Information and System Integrity	293	Chapter Review Questions/Exercises	334
14. Security Assessments	294	Exercise	335
15. Risk Assessments	294	References	335
16. Intranet Security Implementation Process Checklist	295		
17. Summary	295		
Chapter Review Questions/Exercises	296		
Exercise	296		
<b>16. Local Area Network Security (online chapter)</b>	<b>299</b>		
<i>Pramod Pandya</i>			
<b>17. Wireless Network Security</b>	<b>301</b>		
<i>Chunming Rong, Gansen Zhao, Liang Yan, Erdal Cayirci, Hongbing Cheng</i>			
1. Cellular Networks	301		
2. Wireless Ad Hoc Networks	303		
3. Security Protocols	304		
4. Wired Equivalent Privacy	305		
5. Secure Routing	307		
6. Authenticated Routing for Ad Hoc Networks	309		
7. Secure Link State Routing Protocol	309		
8. Key Establishment	310		
9. Ingemarsson, Tang, and Wong	311		
10. Management Countermeasures	313		
11. Summary	314		
Chapter Review Questions/Exercises	314		
Exercise	315		
References	315		
<b>18. Wireless Sensor Network Security: The Internet of Things</b>	<b>317</b>		
<i>Harsh Kupwade Patil, Thomas M. Chen</i>			
1. Introduction to Wireless Sensor Networks	317		
2. Threats to Privacy	319		
3. Cryptographic Security in Wireless Sensor Networks	323		
4. Secure Routing in Wireless Sensor Networks	329		
5. Routing Protocols in Wireless Sensor Networks	330		
6. Wireless Sensor Networks and Internet of Things	332		
7. Summary	334		
		Chapter Review Questions/Exercises	334
		Exercise	335
		References	335
<b>19. Security for the Internet of Things</b>	<b>339</b>		
<i>William Stallings</i>			
1. Introduction	339		
2. ITU-T Internet of Things (IoT) Reference Model	340		
3. Internet of Things (IoT) Security	344		
4. Summary	347		
Chapter Review Questions/Exercises	347		
Exercise	348		
References	348		
<b>20. Cellular Network Security</b>	<b>349</b>		
<i>Peng Liu, Thomas F. LaPorta, Kameswari Kotapati</i>			
1. Introduction	349		
2. Overview of Cellular Networks	349		
3. The State of the Art of Cellular Network Security	352		
4. Cellular Network Attack Taxonomy	354		
5. Cellular Network Vulnerability Analysis	359		
6. Summary	366		
Chapter Review Questions/Exercises	367		
Exercise	367		
References	368		
<b>21. Radio Frequency Identification Security</b>	<b>369</b>		
<i>Chunming Rong, Gansen Zhao, Liang Yan, Erdal Cayirci, Hongbing Cheng</i>			
1. Radio Frequency Identification Introduction	369		
2. Radio Frequency Identification Challenges	372		
3. Radio Frequency Identification Protections	376		
4. Summary	382		
Chapter Review Questions/Exercises	383		
Exercise	383		
References	384		
<b>22. Optical Network Security (online chapter)</b>	<b>387</b>		
<i>Lauren Collins</i>			

## 23. Optical Wireless Security (online chapter) 389

*Scott R. Ellis*

## Part II Managing Information Security 391

### 24. Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems 393

*Albert Caballero*

1. Introduction 393
  2. Protecting Mission-Critical Systems 394
  3. Information Security Essentials for Information Technology Managers 396
  4. Systems and Network Security 399
  5. Application Security 402
  6. Cloud Security 404
  7. Data Protection 407
  8. Wireless and Mobile Security 408
  9. Identity and Access Management 409
  10. Security Operations 410
  11. Policies, Plans, and Programs 413
  12. Summary 417
- Chapter Review Questions/Exercises 417  
Exercise 418  
References 418

### 25. Security Management Systems 421

*Jim Harmening*

1. Security Management System Standards 421
  2. Training Requirements 422
  3. Principles of Information Security 422
  4. Roles and Responsibilities of Personnel 422
  5. Security Policies 422
  6. Security Controls 423
  7. Network Access 423
  8. Risk Assessment 424
  9. Incident Response 425
  10. Summary 425
- Chapter Review Questions/Exercises 426  
Exercise 426

### 26. Policy-Driven System Management 427

*Henrik Plate, Cataldo Basile,  
Stefano Paraboschi*

1. Introduction 427
  2. Security and Policy-Based Management 427
  3. Classification and Languages 439
  4. Controls for Enforcing Security Policies in Distributed Systems 442
  5. Products and Technologies 447
  6. Research Projects 452
  7. Summary 457
- Chapter Review Questions/Exercises 458  
Exercise 458  
Acknowledgments 458  
References 459

### 27. Information Technology Security Management (online chapter) 461

*Rahul Bhaskar, Bhushan Kapoor*

### 28. The Enemy (The Intruder's Genesis) (online chapter) 463

*Pramod Pandya*

### 29. Social Engineering Deceptions and Defenses 465

*Scott R. Ellis*

1. Introduction 465
  2. Counter-Social Engineering 465
  3. Vulnerabilities 466
  4. Using a Layered Defense Approach 467
  5. Attack Scenarios 469
  6. Suspect Everyone: Network Vector 469
  7. Policy and Training 471
  8. Physical Access 472
  9. Summary 472
- Chapter Review Questions/Exercises 473  
Exercise 473

### 30. Ethical Hacking 475

*Scott R. Ellis*

1. Introduction 475
2. Hacker's Toolbox 476

- 3. Attack Vectors 478
- 4. Physical Penetrations 480
- 5. Summary 481
- Chapter Review Questions/Exercises 481
- Exercise 481

### 31. What Is Vulnerability Assessment? 483

*Almantas Kakareka*

- 1. Introduction 483
- 2. Reporting 483
- 3. The “It Will Not Happen to Us” Factor 484
- 4. Why Vulnerability Assessment? 484
- 5. Penetration Testing Versus Vulnerability Assessment 484
- 6. Vulnerability Assessment Goal 485
- 7. Mapping the Network 485
- 8. Selecting the Right Scanners 485
- 9. Central Scans Versus Local Scans 487
- 10. Defense in Depth Strategy 488
- 11. Vulnerability Assessment Tools 488
- 12. Security Auditor’s Research Assistant 489
- 13. Security Administrator’s Integrated Network Tool 489
- 14. Microsoft Baseline Security Analyzer 489
- 15. Scanner Performance 489
- 16. Scan Verification 490
- 17. Scanning Cornerstones 490
- 18. Network Scanning Countermeasures 490
- 19. Vulnerability Disclosure Date 490
- 20. Proactive Security Versus Reactive Security 491
- 21. Vulnerability Causes 492
- 22. Do It Yourself Vulnerability Assessment 493
- 23. Summary 493
- Chapter Review Questions/Exercises 493
- Exercise 494

### 32. Security Metrics: An Introduction and Literature Review (online chapter) 495

*George O.M. Yee*

### 33. Security Education, Training, and Awareness 497

*Albert Caballero*

- 1. Security Education, Training, and Awareness (SETA) Programs 497
- 2. Users, Behavior, and Roles 499
- 3. Security Education, Training, and Awareness (SETA) Program Design 500
- 4. Security Education, Training, and Awareness (SETA) Program Development 501
- 5. Implementation and Delivery 501
- 6. Technologies and Platforms 502
- 7. Summary 503
- Chapter Review Questions/Exercises 504
- Exercise 505
- References 505

### 34. Risk Management 507

*Sokratis K. Katsikas*

- 1. The Concept of Risk 508
- 2. Expressing and Measuring Risk 508
- 3. The Risk Management Methodology 510
- 4. Risk Management Laws and Regulations 522
- 5. Risk Management Standards 524
- 6. Summary 526
- Chapter Review Questions/Exercises 526
- Exercise 527

### 35. Insider Threat 529

*William F. Cross*

- 1. Introduction 529
- 2. Defining Insider Threat 529
- 3. Motivations of the Insider Threat Actors 530
- 4. Insider Threat Indicators 531
- 5. Examples of Insider Threats 531
- 6. Impacts 532
- 7. Analysis: Relevance 532
- 8. Manage and Mitigate the Insider Threat 532
- 9. Summary 534
- Chapter Review Questions/Exercises 535
- Exercise 535
- References 535

## Part III Disaster Recovery Security 537

### 36. Disaster Recovery 539

*Scott R. Ellis, Lauren Collins*

1. Introduction 539
2. Measuring Risk and Avoiding Disaster 539
3. The Business Impact Assessment 541
4. Summary 546
- Chapter Review Questions/Exercises 546
- Exercise 547

### 37. Disaster Recovery Plans for Small and Medium Businesses (SMBs) 549

*William F. Gross, Jr.*

1. Introduction 549
2. Identifying the Need for a Disaster Recovery Plan 549
3. Recovery 549
4. Threat Analysis 550
5. Methodology 550
6. Train and Test the Plan 551
7. Communication 551
8. Recovery 552
9. Summary 552
- Chapter Review Questions/Exercises 552
- Exercise 553
- References 553

## Part IV Security Standards and Policies 555

### 38. Security Certification and Standards Implementation 557

*Keith Lewis*

1. Introduction: The Security Compliance Puzzle 557
2. The Age of Digital Regulations 557
3. Security Regulations and Laws: Technology Challenges 558
4. Implementation: The Compliance Foundation 560
5. Summary 562
- Chapter Review Questions/Exercises 562
- Exercise 563
- References 563

### 39. Security Policies and Plans Development 565

*Keith Lewis*

1. Introduction: Policies and Planning: Security Framework Foundation 565
2. CIA: Not the Central Intelligence Agency 567
3. Security Policy Structure 567
4. Security Policy: Sign Off Approval 569
5. Summary 569
- Chapter Review Questions/Exercises 569
- Exercise 570
- References 570

## Part V Cyber, Network, and Systems Forensics Security and Assurance 571

### 40. Cyber Forensics 573

*Scott R. Ellis*

1. What Is Cyber Forensics? 573
2. Analysis of Data 574
3. Cyber Forensics in the Court System 576
4. Understanding Internet History 577
5. Temporary Restraining Orders and Labor Disputes 578
6. First Principles 589
7. Hacking a Windows XP Password 589
8. Network Analysis 592
9. Cyber Forensics Applied 593
10. Tracking, Inventory, Location of Files, Paperwork, Backups, and So on 593
11. Testifying as an Expert 595
12. Beginning to End in Court 598
13. Summary 601
- Chapter Review Questions/Exercises 601
- Exercise 602

### 41. Cyber Forensics and Incidence Response 603

*Cem Gurkok*

1. Introduction to Cyber Forensics 603
2. Handling Preliminary Investigations 604
3. Controlling an Investigation 606
4. Conducting Disc-Based Analysis 607

5. Investigating Information-Hiding Techniques 610
  6. Scrutinizing Email 614
  7. Validating Email Header Information 615
  8. Tracing Internet Access 616
  9. Searching Memory in Real Time 619
  10. Summary 625
- Chapter Review Questions/Exercises 627  
Exercise 627  
References 628

## 42. Securing e-Discovery 629

*Scott R. Ellis*

1. Information Management 631
  2. Legal and Regulatory Obligation 631
  3. Summary 654
- Chapter Review Questions/Exercises 654  
Exercise 655

## 43. Network Forensics (online chapter) 657

*Yong Guan*

## 44. Microsoft Office and Metadata Forensics: A Deeper Dive 659

*Rich Hoffman*

1. Introduction 659
  2. In a Perfect World 659
  3. Microsoft Excel 660
  4. Exams! 661
  5. Items Outside of Office Metadata 663
  6. Summary 666
- Chapter Review Questions/Exercises 666  
Exercise 667

## 45. Hard Drive Imaging 669

*John Benjamin Khan*

1. Introduction 669
  2. Hard Disc Drives 669
  3. Solid State Drives 669
  4. Hardware Tools 670
  5. Software Tools 670
  6. Techniques 670
  7. Summary 671
- Chapter Review Questions/Exercises 671  
Exercise 672  
References 672

## Part VI Encryption Technology 673

### 46. Data Encryption (online chapter) 675

*Bhushan Kapoor, Pramod Pandya*

### 47. Satellite Encryption 677

*Daniel S. Soper*

1. Introduction 677
  2. The Need for Satellite Encryption 678
  3. Implementing Satellite Encryption 679
  4. Pirate Decryption of Satellite Transmissions 683
  5. Satellite Encryption Policy 685
  6. Satellite Encryption Service (SES) 686
  7. The Future of Satellite Encryption 686
  8. Summary 686
- Chapter Review Questions/Exercises 688  
Exercise 688

### 48. Public Key Infrastructure 691

*Terence Spies*

1. Cryptographic Background 691
2. Overview of Public Key Infrastructure 693
3. The X.509 Model 694
4. X.509 Implementation Architectures 695
5. X.509 Certificate Validation 695
6. X.509 Certificate Revocation 698
7. Server-Based Certificate Validity Protocol 699
8. X.509 Bridge Certification Systems 700
9. X.509 Certificate Format 702
10. Public Key Infrastructure Policy Description 704
11. Public Key Infrastructure Standards Organizations 705
12. Pretty Good Privacy Certificate Formats 706
13. Pretty Good Privacy Public Key Infrastructure Implementations 706
14. World Wide Web Consortium 707
15. Is Public Key Infrastructure Secure? 707
16. Alternative Public Key Infrastructure Architectures 707
17. Modified X.509 Architectures 708

18. Alternative Key Management Models 708
19. Summary 709
- Chapter Review Questions/Exercises 710
- Exercise 710
- References 710
- 49. Password-Based Authenticated Key Establishment Protocols (online chapter) 713**
- Jean Lancrenon, Dalia Khader, Peter Y.A. Ryan, Feng Hao*
- 50. Context-Aware Multifactor Authentication Survey 715**
- Emin Huseynov, Jean-Marc Seigneur*
1. Introduction 715
  2. Classic Approach to Multifactor Authentication 715
  3. Modern Approaches to Multifactor Authentication 718
  4. Comparative Summary 722
  5. Summary 723
- Chapter Review Questions/Exercises 724
- Exercise 726
- References 726
- 51. Instant-Messaging Security 727**
- Samuel J.J. Curry*
1. Why Should I Care About Instant Messaging? 727
  2. What Is Instant Messaging? 727
  3. The Evolution of Networking Technologies 728
  4. Game Theory and Instant Messaging 728
  5. The Nature of the Threat 731
  6. Common Instant Messaging Applications 734
  7. Defensive Strategies 735
  8. Instant-Messaging Security Maturity and Solutions 736
  9. Processes 737
  10. Summary 738
- Chapter Review Questions/Exercises 740
- Exercise 740

## Part VII Privacy and Access Management 741

### 52. Online Privacy 743

*Chiara Braghin, Marco Cremonini*

1. The Quest for Privacy 743
  2. Trading Personal Data 746
  3. Control of Personal Data 747
  4. Privacy and Technologies 749
  5. Summary 755
- Chapter Review Questions/Exercises 755
- Exercise 756
- References 756

### 53. Privacy-Enhancing Technologies 759

*Simone Fischer-Hbner, Stefan Berthold*

1. The Concept of Privacy 759
  2. Legal Privacy Principles 759
  3. Classification of Privacy-Enhancing Technologies (PETs) 761
  4. Traditional Privacy Goals of Privacy-Enhancing Technologies (PETs) 761
  5. Privacy Metrics 762
  6. Data Minimization Technologies 764
  7. Transparency-Enhancing Tools 772
  8. Summary 775
- Chapter Review Questions/Exercises 775
- Exercise 776
- References 776

### 54. Personal Privacy Policies (online chapter) 779

*George O.M. Yee, Larry Korba*

### 55. Detection of Conflicts in Security Policies 781

*Cataldo Basile, Matteo Maria Casalino, Simone Mutti, Stefano Paraboschi*

1. Introduction 781
2. Conflicts in Security Policies 781

- 3. Conflicts in Executable Security Policies 785
  - 4. Conflicts in Network Security Policies 788
  - 5. Query-Based Conflict Detection 789
  - 6. Semantic Web Technology for Conflict Detection 795
  - 7. Summary 798
  - Chapter Review Questions/Exercises 798
  - Exercise 799
  - Acknowledgments 799
  - References 799
- 56. Supporting User Privacy Preferences in Digital Interactions 801**
- Sara Foresti, Pierangela Samarati*
- 1. Introduction 801
  - 2. Basic Concepts and Desiderata 802
  - 3. Cost-Sensitive Trust Negotiation 805
  - 4. Point-Based Trust Management 808
  - 5. Logical-Based Minimal Credential Disclosure 810
  - 6. Privacy Preferences in Credential-Based Interactions 812
  - 7. Fine-Grained Disclosure of Sensitive Access Policies 817
  - 8. Open Issues 819
  - 9. Summary 819
  - Chapter Review Questions/Exercises 820
  - Exercise 820
  - Acknowledgments 820
  - References 821
- 57. Privacy and Security in Environmental Monitoring Systems: Issues and Solutions 823**
- Sabrina De Capitani di Vimercati, Angelo Genovese, Giovanni Livraga, Vincenzo Piuri, Fabio Scotti*
- 1. Introduction 823
  - 2. System Architectures 824
  - 3. Environmental Data 826
  - 4. Security and Privacy Issues in Environmental Monitoring 827
  - 5. Countermeasures 829
  - 6. Summary 838
  - Chapter Review Questions/Exercises 838
  - Exercise 838
  - Acknowledgments 839
  - References 839
- 58. Virtual Private Networks 843**
- James T. Harmening*
- 1. History 844
  - 2. Who Is in Charge? 847
  - 3. Virtual Private Network Types 848
  - 4. Authentication Methods 851
  - 5. Symmetric Encryption 851
  - 6. Asymmetric Cryptography 852
  - 7. Edge Devices 852
  - 8. Passwords 852
  - 9. Hackers and Crackers 853
  - 10. Mobile Virtual Private Network 853
  - 11. Virtual Private Network Deployments 854
  - 12. Summary 854
  - Chapter Review Questions/Exercises 854
  - Exercise 855
  - References 856
  - Resources 856
- 59. Identity Theft (online chapter) 857**
- Markus Jakobsson, Alex Tsow*
- 60. VoIP Security 859**
- Harsh Kupwade Patil, Dan Wing, Thomas M. Chen*
- 1. Introduction 859
  - 2. Overview of Threats 861
  - 3. Security in Voice Over Internet Protocol 866
  - 4. Future Trends 868
  - 5. Summary 871
  - Chapter Review Questions/Exercises 872
  - Exercise 873
- Part VIII**
- Storage Security 875**
- 61. SAN Security (online chapter) 877**
- John McGowan, Jeffrey S. Bardin, John McDonald*
- 62. Storage Area Networking Security Devices 879**
- Robert Rounsavall*
- 1. What Is Storage Area Networking (SAN)? 879
  - 2. Storage Area Networking (SAN) Deployment Justifications 879

3. The Critical Reasons for Storage Area Networking (SAN) Security 880
4. Storage Area Networking (SAN) Architecture and Components 880
5. Storage Area Networking (SAN) General Threats and Issues 882
6. Summary 893
- Chapter Review Questions/Exercises 893
- Exercise 894

## Part IX Cloud Security 895

### 63. Securing Cloud Computing Systems 897

*Cem Gurkok*

1. Cloud Computing Essentials: Examining the Cloud Layers 897
2. Software as a Service: Managing Risks in the Cloud 903
3. Platform as a Service: Securing the Platform 904
4. Infrastructure as a Service 907
5. Leveraging Provider-Specific Security Options 911
6. Achieving Security in a Private Cloud 912
7. Meeting Compliance Requirements 916
8. Preparing for Disaster Recovery 919
9. Summary 921
- Chapter Review Questions/Exercises 921
- Exercise 922
- References 922

### 64. Cloud Security 923

*Edward G. Amoroso*

1. Cloud Overview: Public, Private, Hybrid 923
2. Cloud Security Threats 924
3. Internet Service Provider Cloud Virtual Private Network Peering Services 924
4. Cloud Access Security Brokers 925
5. Cloud Encryption 925
6. Cloud Security Microsegmentation 926
7. Cloud Security Compliance 927
8. Summary 929
- Chapter Review Questions/Exercises 929
- Exercise 929
- References 930

### 65. Private Cloud Security 931

*Keith Lewis*

1. Introduction: Private Cloud System Management 931
2. From Physical to Network Security Base Focus 931
3. Benefits of Private Cloud Security Infrastructures 933
4. Private Cloud Security Standards and Best Practices 933
5. "As-a-Service" Universe: Service Models 934
6. Private Cloud Service Model: Layer Considerations 935
7. Privacy or Public: The Cloud Security Challenges 935
8. Summary 935
- Chapter Review Questions/Exercises 936
- Exercise 936
- References 936

### 66. Virtual Private Cloud Security 937

*Keith Lewis*

1. Introduction: Virtual Networking in a Private Cloud 937
2. Security Console: Centralized Control Dashboard Management 937
3. Security Designs: Virtual Private Cloud Setups 938
4. Security Object Group Allocations: Functional Control Management Practices 939
5. Virtual Private Cloud Performance Versus Security 940
6. Summary 941
- Chapter Review Questions/Exercises 941
- Exercise 942
- References 942

## Part X Virtual Security 943

### 67. Protecting Virtual Infrastructure 945

*Edward G. Amoroso*

1. Virtualization in Computing 945
2. Virtual Data Center Security 946
3. Hypervisor Security 947
4. Enterprise Segmentation 947

5. Active Containerized Security 948
6. Virtual Absorption of Volume Attacks 948
7. Open Source Versus Proprietary Security Capabilities 949
8. Summary 950
- Chapter Review Questions/Exercises 950
- Exercise 951
- Reference 951

## 68. Software-Defined Networking and Network Function Virtualization Security 953

*Edward G. Amoroso*

1. Introduction to Software-Defined Networking 953
2. Software-Defined Networking and Network Function Virtualization Overview 954
3. Software-Defined Networking and Network Function Virtualization for Internet Service Providers 956
4. Software-Defined Networking Controller Security 956
5. Improved Patching With Software-Defined Networking 957
6. Dynamic Security Service Chaining in Software-Defined Networking 957
7. Future Virtualized Management Security Support in Software-Defined Networking 959
8. Summary 959
- Chapter Review Questions/Exercises 960
- Exercise 961
- References 961

## Part XI Cyber Physical Security 963

### 69. Physical Security Essentials 965

*William Stallings*

1. Overview 965
2. Physical Security Threats 966
3. Physical Security Prevention and Mitigation Measures 970
4. Recovery From Physical Security Breaches 971

5. Threat Assessment, Planning, and Plan Implementation 971
6. Example: A Corporate Physical Security Policy 972
7. Integration of Physical and Logical Security 973
8. Physical Security Checklist 976
9. Summary 976
- Chapter Review Questions/Exercises 977
- Exercise 979
- References 979

### 70. Biometrics (online chapter) 981

*Luther Martin*

## Part XII Practical Security 983

### 71. Online Identity and User Management Services 985

*Tewfiq El Maliki, Jean-Marc Seigneur*

1. Introduction 985
2. Evolution of Identity Management Requirements 985
3. The Requirements Fulfilled by Identity Management Technologies 989
4. Identity Management 1.0 989
5. Social Login and User Management 1001
6. Identity 2.0 for Mobile Users 1002
7. Summary 1007
- Chapter Review Questions/Exercises 1007
- Exercise 1008
- References 1008

### 72. Intrusion Prevention and Detection Systems 1011

*Christopher Day*

1. What Is an “Intrusion” Anyway? 1011
2. Physical Theft 1011
3. Abuse of Privileges (the Insider Threat) 1011
4. Unauthorized Access by Outsider 1012
5. Malicious Software Infection 1012
6. Role of the “Zero-Day” 1013

- 7. The Rogue's Gallery: Attackers and Motives 1014
  - 8. A Brief Introduction to Transmission Control Protocol/Internet Protocol 1014
  - 9. Transmission Control Protocol/Internet Protocol Data Architecture and Data Encapsulation 1015
  - 10. Survey of Intrusion Detection and Prevention Technologies 1019
  - 11. Antimalicious Software 1019
  - 12. Network-Based Intrusion Detection Systems 1019
  - 13. Network-Based Intrusion Prevention Systems 1021
  - 14. Host-Based Intrusion Prevention Systems 1021
  - 15. Security Information Management Systems 1021
  - 16. Network Session Analysis 1022
  - 17. Digital Forensics 1023
  - 18. System Integrity Validation 1023
  - 19. Summary 1023
  - Chapter Review Questions/Exercises 1023
  - Exercise 1024
  - References 1024
- 73. Transmission Control Protocol/Internet Protocol Packet Analysis (online chapter) 1027**  
*Pramod Pandya*
- 74. Firewalls (online chapter) 1029**  
*Errin W. Fulp*
- 75. Penetration Testing 1031**  
*Roman Zabicki, Scott R. Ellis*
- 1. What Is Penetration Testing? 1031
  - 2. Why Would You Do It? 1031
  - 3. How Do You Do It? 1032
  - 4. Examples of Penetration Test Scenarios 1035
  - 5. Summary 1037
  - Chapter Review Questions/Exercises 1037
  - Exercise 1038
  - References 1038
- 76. System Security (online chapter) 1039**  
*Lauren Collins*
- 77. Access Controls 1041**  
*Lauren Collins*
- 1. Infrastructure Weaknesses: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) 1041
  - 2. Strengthening the Infrastructure: Authentication Systems 1044
  - 3. Summary 1046
  - Chapter Review Questions/Exercises 1047
  - Exercise 1047
- 78. Endpoint Security 1049**  
*Keith Lewis*
- 1. Introduction: Endpoint Security Defined 1049
  - 2. Endpoint Solution: Options 1049
  - 3. Standard Requirements: Security Decisions 1049
  - 4. Endpoint Architecture: Functional Challenges 1050
  - 5. Endpoint Intrusion Security: Management Systems 1052
  - 6. Intrusion Prevention System (IPS) Network Logging Tools: Seek and Target (the Offender) 1053
  - 7. Endpoint Unification: Network Access Control (NAC) Design Approach (From the Ground-Up) 1053
  - 8. Software-as-a-Service (SaaS) Endpoint Security 1053
  - 9. Summary 1054
  - Chapter Review Questions/Exercises 1054
  - Exercise 1055
  - References 1055
- 79. Assessments and Audits (online chapter) 1057**  
*Lauren Collins*

**80. Fundamentals of  
Cryptography 1059**

*Scott R. Ellis*

- 1. Assuring Privacy With Encryption 1059
- 2. Summary 1065
- Chapter Review Questions/Exercises 1065
- Exercise 1066

**Part XIII**

**Critical Infrastructure Security 1067**

**81. Securing the Infrastructure 1069**

*Lauren Collins*

- 1. Communication Security Goals 1069
- 2. Attacks and Countermeasures 1076
- 3. Summary 1080
- Chapter Review Questions/Exercises 1081
- Exercise 1081

**82. Homeland Security  
(online chapter) 1083**

*Rahul Bhaskar, Bhushan Kapoor*

**83. Cyber Warfare 1085**

*Anna Granova, Marco Slaviero*

- 1. Cyber Warfare Model 1085
- 2. Cyber Warfare Defined 1086
- 3. Cyber Warfare: Myth or Reality? 1086
- 4. Participants, Roles, Attribution, and Asymmetry 1088
- 5. Making Cyber Warfare Possible 1092
- 6. Legal Aspects of Cyber Warfare 1099
- 7. Holistic View of Cyber Warfare 1103
- 8. Summary 1103
- Chapter Review Questions/Exercises 1103
- Exercise 1104

**84. Cyber-Attack Process 1105**

*Nailah Mims*

- 1. What Is a Cyber-Attack? 1105
- 2. Cyber-Attack Adversaries 1106
- 3. Cyber-Attack Targets 1106
- 4. Cyber-Attack Process 1106
- 5. Tools and Tactics of a Cyber-Attack 1107
- 6. Cyber-Attack Case Studies 1110

- 7. Advanced Persistent Threat 1113
- 8. Additional Considerations 1114
- 9. Summary 1114
- Chapter Review Questions/Exercises 1115
- Exercise 1115
- References 1116

**Part XIV**

**Advanced Security 1117**

**85. Security Through Diversity 1119**

*Kevin Noble*

- 1. Ubiquity 1120
- 2. Example Attacks Against Uniformity 1121
- 3. Attacking Ubiquity With Antivirus Tools 1122
- 4. The Threat of Worms 1122
- 5. Automated Network Defense 1124
- 6. Diversity and the Browser 1125
- 7. Sandboxing and Virtualization 1126
- 8. Domain Name Server Example of Diversity Through Security 1126
- 9. Recovery From Disaster Is Survival 1127
- 10. Summary 1127
- Chapter Review Questions/Exercises 1128
- Exercise 1129

**86. e-Reputation and Online  
Reputation Management  
Survey 1131**

*Jean-Marc Seigneur*

- 1. Introduction 1131
- 2. The Human Notion of Reputation 1132
- 3. Reputation Applied to the Computing World 1134
- 4. State of the Art of Attack-Resistant Reputation Computation 1137
- 5. Overview of Past and Current Online Reputation Services 1141
- 6. Summary 1149
- Chapter Review Questions/Exercises 1150
- Exercise 1150
- References 1150

**87. Content Filtering  
(online chapter) 1153**

*Pete F. Nicoletti*

**88. Data Loss Protection 1155***Ken Perkins*

1. Precursors of DLP 1156
  2. What Is Data Loss Protection (DLP)? 1157
  3. Where to Begin? 1162
  4. Data Is Like Water 1162
  5. You Don't Know What You Don't Know 1164
  6. How Do Data Loss Protection (DLP) Applications Work? 1165
  7. Eat Your Vegetables 1166
  8. IT's a Family Affair, Not Just IT Security's Problem 1169
  9. Vendors, Vendors Everywhere! Who Do You Believe? 1169
  10. Summary 1170
- Chapter Review Questions/Exercises 1171  
Exercise 1171

**89. Satellite Cyber Attack Search and Destroy 1173***Jeffrey Bardin*

1. Hacks, Interference, and Jamming 1173
2. Summary 1180

- Chapter Review Questions/Exercises 1180  
Exercise 1181  
References 1181

**90. Verifiable Voting Systems (online chapter) 1183***Thea Peacock, Peter Y.A. Ryan, Steve Schneider, Zhe Xia***91. Advanced Data Encryption 1185***Pramod Pandya*

1. Mathematical Concepts Reviewed 1185
  2. The Rivest, Shamir, and Adelman Cryptosystem 1189
  3. Summary 1194
- Chapter Review Questions/Exercises 1195  
Exercise 1195  
References 1195

Index 1197

**Online Chapters and Appendices****16. Local Area Network Security e1***Pramod Pandya*

1. Identify Network Threats e1
2. Establish Network Access Controls e2
3. Risk Assessment e3
4. Listing Network Resources e3
5. Threats e3
6. Security Policies e4
7. The Incident-Handling Process e4
8. Secure Design Through Network Access Controls e4
9. Intrusion Detection System Defined e5
10. Network Intrusion Detection System: Scope and Limitations e5
11. A Practical Illustration of Network Intrusion Detection System e5
12. Firewalls e7

13. Dynamic Network Address Translation Configuration e11
  14. The Perimeter e11
  15. Access List Details e13
  16. Types of Firewalls e14
  17. Packet Filtering: Internet Protocol Filtering Routers e14
  18. Application-Layer Firewalls: Proxy Servers e14
  19. Stateful Inspection Firewalls e14
  20. Network Intrusion Detection System Complements Firewalls e14
  21. Monitor and Analyze System Activities e15
  22. Signature Analysis e15
  23. Statistical Analysis e15
  24. Signature Algorithms e16
  25. Local Area Network Security Countermeasures Implementation Checklist e19
  26. Summary e19
- Chapter Review Questions/Exercises e19  
Exercise e20

**22. Optical Network Security e21**

*Lauren Collins*

1. Optical Networks e21
  2. Securing Optical Networks e23
  3. Identifying Vulnerabilities e25
  4. Corrective Actions e26
  5. Summary e26
- Chapter Review Questions/Exercises e27  
Exercise e27  
References e27

**23. Optical Wireless Security e29**

*Scott R. Ellis*

1. Optical Wireless Systems Overview e29
  2. Deployment Architectures e30
  3. High Bandwidth e31
  4. Low Cost e31
  5. Implementation e31
  6. Surface Area e31
  7. Summary e33
- Chapter Review Questions/Exercises e33  
Exercise e34

**27. Information Technology Security Management e35**

*Rahul Bhaskar, Bhushan Kapoor*

1. Information Security Management Standards e35
  2. Other Organizations Involved in Standards e36
  3. Information Technology Security Aspects e36
  4. Summary e43
- Chapter Review Questions/Exercises e43  
Exercise e44

**28. The Enemy (The Intruder's Genesis) e45**

*Pramod Pandya*

1. Introduction e45
  2. Active Reconnaissance e46
  3. Enumeration e50
  4. Penetration and Gain Access e51
  5. Maintain Access e53
  6. Defend Network Against Unauthorized Access e54
  7. Summary e55
- Chapter Review Questions/Exercises e55  
Exercise e56

**32. Security Metrics: An Introduction and Literature Review e57**

*George O.M. Yee*

1. Introduction e57
  2. Why Security Metrics? e58
  3. The Nature of Security Metrics e59
  4. Getting Started With Security Metrics e62
  5. Metrics in Action: Toward an Intelligent Security Dashboard e63
  6. Security Metrics in the Literature e63
  7. Summary e68
- Chapter Review Questions/Exercises e69  
Exercise e69  
References e69

**43. Network Forensics e71**

*Yong Guan*

1. Scientific Overview e71
  2. The Principles of Network Forensics e71
  3. Attack Trace-Back and Attribution e72
  4. Critical Needs Analysis e78
  5. Research Directions e78
  6. Summary e79
- Chapter Review Questions/Exercises e81  
Exercise e82

**46. Data Encryption e83**

*Bhushan Kapoor, Pramod Pandya*

1. Need for Cryptography e83
2. Mathematical Prelude to Cryptography e84
3. Classical Cryptography e84
4. Modern Symmetric Ciphers e87
5. Algebraic Structure e89
6. The Internal Functions of Rijndael in Advanced Encryption Standard Implementation e93
7. Use of Modern Block Ciphers e97
8. Public-Key Cryptography e98
9. Cryptanalysis of Rivest–Shamir–Adleman e101
10. Diffie–Hellman Algorithm e102
11. Elliptic Curve Cryptosystems e102
12. Message Integrity and Authentication e104
13. Triple Data Encryption Algorithm Block Cipher e105
14. Summary e106

- Chapter Review Questions/Exercises e106  
Exercise e107  
References e107
- 49. Password-Based Authenticated Key Establishment Protocols e109**  
*Jean Lancrenon, Dalia Khader, Peter Y.A. Ryan, Feng Hao*
1. Introduction to Key Exchange e109
  2. Password-Authenticated Key Exchange e112
  3. Concrete Protocols e114
  4. Summary e121
- Chapter Review Questions/Exercises e121  
Exercise e122  
References e122
- 54. Personal Privacy Policies e125**  
*George O.M. Yee, Larry Korba*
1. Introduction e125
  2. Content of Personal Privacy Policies e126
  3. Semiautomated Derivation of Personal Privacy Policies e127
  4. Specifying Well-Formed Personal Privacy Policies e131
  5. Preventing Unexpected Negative Outcomes e134
  6. The Privacy Management Model e135
  7. Discussion and Related Work e140
  8. Summary e142
- Chapter Review Questions/Exercises e143  
Exercise e143
- 59. Identity Theft e145**  
*Markus Jakobsson, Alex Tsow*
1. Experimental Design e145
  2. Results and Analysis e152
  3. Implications for Crimeware e160
- Chapter Review Questions/Exercises e162  
Exercise e163  
References e163
- 61. SAN Security e165**  
*John McGowan, Jeffrey S. Bardin, John McDonald*
1. Organizational Structure e165
  2. Access Control Lists and Policies e167
  3. Physical Access e168
  4. Change Management e168
  5. Password Policies e168
  6. Defense-in-Depth e169
  7. Vendor Security Review e169
  8. Data Classification e169
  9. Security Management e169
  10. Auditing e169
  11. Security Maintenance e170
  12. Host Access: Partitioning e171
  13. Data Protection: Replicas e172
  14. Encryption in Storage e174
  15. Application of Encryption e177
  16. Summary e185
- Chapter Review Questions/Exercises e185  
Exercise e187  
Reference e187
- 70. Biometrics e189**  
*Luther Martin*
1. Relevant Standards e190
  2. Biometric System Architecture e191
  3. Using Biometric Systems e197
  4. Security Considerations e199
  5. Summary e203
- Chapter Review Questions/Exercises e203  
Exercise e204
- 73. Transmission Control Protocol/Internet Protocol Packet Analysis e205**  
*Pramod Pandya*
1. The Internet Model e205
  2. Summary e218
- Chapter Review Questions/Exercises e218  
Exercise e218
- 74. Firewalls e219**  
*Errin W. Fulp*
1. Introduction e219
  2. Network Firewalls e219
  3. Firewall Security Policies e220
  4. A Simple Mathematical Model for Policies, Rules, and Packets e221
  5. First-Match Firewall Policy Anomalies e222
  6. Policy Optimization e222
  7. Firewall Types e223
  8. Host and Network Firewalls e225
  9. Software and Hardware Firewall Implementations e225

- 10. Choosing the Correct Firewall e225
- 11. Firewall Placement and Network Topology e226
- 12. Firewall Installation and Configuration e228
- 13. Supporting Outgoing Services Through Firewall Configuration e228
- 14. Secure External Services Provisioning e230
- 15. Network Firewalls for Voice and Video Applications e230
- 16. Firewalls and Important Administrative Service Protocols e231
- 17. Internal IP Services Protection e232
- 18. Firewall Remote Access Configuration e233
- 19. Load Balancing and Firewall Arrays e234
- 20. Highly Available Firewalls e235
- 21. Firewall Management e236
- 22. Summary e236
- Chapter Review Questions/Exercises e237
- Exercise e237

## 76. System Security e239

*Lauren Collins*

- 1. Foundations of Security e239
- 2. Basic Countermeasures e243
- 3. Summary e245
- Chapter Review Questions/Exercises e246
- Exercise e246

## 79. Assessments and Audits e247

*Lauren Collins*

- 1. Assessing Vulnerabilities and Risk: Penetration Testing and Vulnerability Assessments e247
- 2. Risk Management: Quantitative Risk Measurements e251
- 3. Summary e252
- Chapter Review Questions/Exercises e254
- Exercise e254

## 82. Homeland Security e255

*Rahul Bhaskar, Bhushan Kapoor*

- 1. Statutory Authorities e255
- 2. Homeland Security Presidential Directives e261
- 3. Organizational Actions e262
- 4. Summary e267
- Chapter Review Questions/Exercises e268
- Exercise e269

## 87. Content Filtering e271

*Pete F. Nicoletti*

- 1. Defining the Problem e271
- 2. Why Content Filtering Is Important e272
- 3. Content Categorization Technologies e274
- 4. Perimeter Hardware and Software Solutions e276
- 5. Categories e279
- 6. Legal Issues e280
- 7. Circumventing Content Filtering e284
- 8. Additional Items to Consider: Overblocking and Underblocking e286
- 9. Related Products e289
- 10. Summary e289
- Chapter Review Questions/Exercises e291
- Exercise e291

## 90. Verifiable Voting Systems e293

*Thea Peacock, Peter Y.A. Ryan, Steve Schneider, Zhe Xia*

- 1. Introduction e293
- 2. Security Requirements e293
- 3. Verifiable Voting Schemes e295
- 4. Building Blocks e296
- 5. Survey of Noteworthy Schemes e304
- 6. Threats to Verifiable Voting Systems e311
- 7. Summary e312
- Chapter Review Questions/Exercises e312
- Exercise e313
- References e313

## Part XV Appendices e317

- Appendix A Configuring Authentication Service On Microsoft Windows 10 e319
- Appendix B Security Management and Resiliency e323
- Appendix C List of Top Information and Network Security Implementation and Deployment Companies e325
- Appendix D List of Security Products e329
- Appendix E List of Security Standards e343
- Appendix F List of Miscellaneous Security Resources e345

Appendix G	Ensuring Built-in, Frequency-Hopping Spread- Spectrum, Wireless Network Security e355	Appendix J	Case Studies e365
Appendix H	Configuring Wireless Security Remote Access e357	Appendix K	Answers to Review Questions/Exercises, Hands-on Projects, Case Projects and Optional Team Case Project by Chapter e381
Appendix I	Frequently Asked Questions e363	Appendix L	Glossary e471