

Contents

Preface.....	xix
---------------------	------------

Part I: Understanding Computer Network Security

1. Computer Network Fundamentals.....	3
1.1 Introduction	3
1.2 Computer Network Models	4
1.3 Computer Network Types	5
1.3.1 Local Area Network (LANs)	5
1.3.2 Wide Area Networks (WANs).....	6
1.3.3 Metropolitan Area Networks (MANs).....	7
1.4 Data Communication Media Technology.....	8
1.4.1 Transmission Technology	8
1.4.2 Transmission Media.....	11
1.5 Network Topology.....	15
1.5.1 Mesh.....	15
1.5.2 Tree	15
1.5.3 Bus	16
1.5.4 Star	17
1.5.5 Ring.....	18
1.6 Network Connectivity and Protocols.....	19
1.6.1 Open System Interconnection (OSI) Protocol Suite	20
1.6.2 Transport Control Protocol/Internet Protocol (TCP/IP) Model.	22
1.7 Network Services.....	26
1.7.1 Connection Services.....	26
1.7.2 Network Switching Services.....	27
1.8 Network Connecting Devices.....	30
1.8.1 LAN Connecting Devices	30
1.8.2 Internetworking Devices.....	34
1.9 Network Technologies.....	39
1.9.1 LAN Technologies.....	39
1.9.2 WAN Technologies	42
1.9.3 Wireless LANs.....	45
1.10 Conclusion.....	46
1.11 References	46

1.12 Exercises.....	46
1.13 Advanced Exercises.....	47
2. Understanding Network Security	49
2.1 What Is Network Security?	49
2.1.1 Physical Security.....	50
2.1.2 Pseudosecurity	52
2.2 What are we protecting?.....	53
2.2.1 Hardware.....	53
2.2.2 Software	53
2.3 Security Services	54
2.3.1 Access Control	54
2.3.2 Authentication.....	55
2.3.3 Confidentiality	57
2.3.4 Integrity	58
2.3.5 Non-repudiation	58
2.4 Security Standards	59
2.4.1 Security Standards Based on Type of Service/Industry.....	60
2.4.2 Security Standards Based on Size/Implementation	64
2.4.3 Security Standards Based on Interests	65
2.4.4 Best Practices in Security.....	67
2.5 Elements of Security.....	69
2.5.1 The Security Policy.....	69
2.5.2 Access Control	70
2.5.3 Strong Encryption Algorithms.....	70
2.5.4 Authentication Techniques	70
2.5.5 Auditing	72
2.6 References	72
2.7 Exercises.....	72
2.8 Advanced Exercises.....	73

Part II: Security Challenges to Computer Networks

3. Security Threats to Computer Networks.....	77
3.1 Introduction	77
3.2 Sources of Security Threats.....	79
3.2.1 Design Philosophy	79
3.2.2 Weaknesses in Network Infrastructure and Communication Protocols.....	80

3.2.3	Rapid Growth of Cyberspace	84
3.2.4	The Growth of the Hacker Community	85
3.2.5	Vulnerability in Operating System Protocol	95
3.2.6	The Invisible Security Threat -The Insider Effect	95
3.2.7	Social Engineering	96
3.2.8	Physical Theft.....	97
3.3	Security Threat Motives	97
3.3.1	Terrorism.....	97
3.3.2	Military Espionage.....	98
3.3.3	Economic Espionage.....	98
3.3.4	Targeting the National Information Infrastructure.....	99
3.3.5	Vendetta/Revenge	99
3.3.6	Hate (national origin, gender, and race).....	100
3.3.7	Notoriety	100
3.3.8	Greed.....	100
3.3.9	Ignorance.....	100
3.4	Security Threat Management.....	100
3.4.1	Risk Assessment.....	101
3.4.2	Forensic Analysis	101
3.5	Security Threat Correlation	101
3.5.1	Threat Information Quality	102
3.6	Security Threat Awareness.....	103
3.7	References.....	104
3.8	Exercises.....	105
3.9	Advanced Exercises.....	106

4. Computer Network Vulnerabilities..... 109

4.1	Definition.....	109
4.2	Sources of Vulnerabilities.....	109
4.2.1	Design Flaws	110
4.2.2	Poor Security Management	114
4.2.3	Incorrect Implementation	115
4.2.4	Internet Technology Vulnerability	117
4.2.5	Changing Nature of Hacker Technologies and Activities....	120
4.2.6	Difficulty of Fixing Vulnerable Systems	122
4.2.7	Limits of Effectiveness of Reactive Solutions	122
4.2.8	Social Engineering	124
4.3	Vulnerability Assessment	126
4.3.1	Vulnerability Assessment Services	126
4.3.2	Advantages of Vulnerability Assessment Services	128
4.4	References.....	128
4.5	Exercises	129
4.6	Advanced Exercises.....	129

5. Cyber Crimes and Hackers.....	131
5.1 Introduction.....	131
5.2 Cyber Crimes	132
5.2.1 Ways of Executing Cyber Crimes	133
5.2.2 Cyber Criminals	136
5.3 Hackers	137
5.3.1 History of Hacking	138
5.3.2 Types of Hackers.....	141
5.3.3 Hacker Motives	145
5.3.4 Hacking Topologies	149
5.3.5 Hackers' Tools of System Exploitation.....	153
5.3.6 Types of Attacks.....	157
5.4 Dealing with the Rising Tide of Cyber Crimes	158
5.4.1 Prevention.....	158
5.4.2 Detection	159
5.4.3 Recovery.....	159
5.5 Conclusion	160
5.6 References.....	160
5.7 Exercises	162
5.8 Advanced Exercises.....	162
6. Hostile Scripts.....	163
6.1 Introduction	163
6.2 Introduction to the Common Gateway Interface (CGI).....	164
6.3 CGI Scripts in a Three-Way Handshake	165
6.4 Server – CGI Interface.....	167
6.5 CGI Script Security Issues.....	168
6.6 Web Script Security Issues.....	170
6.7 Dealing with the Script Security Problems.....	170
6.8 Scripting Languages	171
6.8.1 Server-Side Scripting Languages	171
6.8.2 Client-Side Scripting Languages.....	173
6.9 References	175
6.10 Exercises.....	175
6.11 Advanced Exercises.....	175
7. Security Assessment, Analysis, and Assurance	177
7.1 Introduction.....	177
7.2 System Security Policy	178
7.3 Building a Security Policy	181

7.3.1	Security Policy Access Rights Matrix	182
7.3.2	Policy and Procedures.....	185
7.4	Security Requirements Specification.....	189
7.5	Threat Identification.....	190
7.5.1	Human Factors.....	191
7.5.2	Natural Disasters.....	192
7.5.3	Infrastructure Failures.....	192
7.6	Threat Analysis	195
7.6.1	Approaches to Security Threat Analysis	196
7.7	Vulnerability Identification and Assessment	197
7.7.1	Hardware.....	197
7.7.2	Software.....	197
7.7.3	Humanware.....	199
7.7.4	Policies, Procedures, and Practices.....	200
7.8	Security Certification.....	201
7.8.1	Phases of a Certification Process	201
7.8.2	Benefits of Security Certification	202
7.9	Security Monitoring and Auditing	202
7.9.1	Monitoring Tools	203
7.9.2	Type of Data Gathered.....	204
7.9.3	Analyzed Information.....	204
7.9.4	Auditing	205
7.10	Products and Services	205
7.11	References.....	206
7.12	Exercises	206
7.13	Advanced Exercises	207

Part III: Dealing with Network Security Challenges

8. Access Control and Authorization 209

8.1	Definitions.....	209
8.2	Access Rights	210
8.2.1	Access Control Techniques and Technologies.....	212
8.3	Access Control Systems	218
8.3.1	Physical Access Control.....	218
8.3.2	Access Cards	218
8.3.3	Electronic Surveillance	219
8.3.4	Biometrics	220
8.3.5	Event Monitoring	223
8.4	Authorization.....	224
8.4.1	Authorization Mechanisms.....	225
8.5	Types of Authorization Systems	226
8.5.1	Centralized	226

8.5.2	Decentralized.....	227
8.5.3	Implicit	227
8.5.4	Explicit	227
8.6	Authorization Principles.....	228
8.6.1	Least Privileges	228
8.6.2	Separation of Duties	228
8.7	Authorization Granularity	229
8.7.1	Fine Grain Authorization	229
8.7.2	Coarse Grain Authorization	229
8.8	Web Access and Authorization	230
8.9	References	231
8.10	Exercises.....	231
8.11	Advanced Exercises	232
9. Authentication		233
9.1	Definition	233
9.2	Multiple Factors and Effectiveness of Authentication.....	235
9.3	Authentication Elements	237
9.3.1	Person or Group Seeking Authentication	237
9.3.2	Distinguishing Characteristics for Authentication.....	237
9.3.3	The Authenticator	238
9.3.4	The Authentication Mechanism.....	238
9.3.5	Access Control Mechanism	239
9.4	Types of Authentication.....	239
9.4.1	Non-repudiable Authentication	239
9.4.2	Repudiable Authentication	241
9.5	Authentication Methods.....	241
9.5.1	Password Authentication	241
9.5.2	Public Key Authentication.....	245
9.5.3	Remote Authentication	249
9.5.4	Anonymous Authentication	251
9.5.5	Digital Signatures-Based Authentication	251
9.5.6	Wireless Authentication.....	252
9.6	Developing an Authentication Policy	252
9.7	References.....	254
9.8	Exercises	255
9.9	Advanced Exercises	255
10. Cryptography		257
10.1	Definition.....	257
10.1.1	Block Ciphers.....	259

10.2 Symmetric Encryption	261
10.2.1 Symmetric Encryption Algorithms	262
10.2.2 Problems with Symmetric Encryption	264
10.3 Public Key Encryption.....	265
10.3.1 Public Key Encryption Algorithms	268
10.3.2 Problems with Public Key Encryption	268
10.3.3 Public Key Encryption Services.....	269
10.4 Enhancing Security: Combining Symmetric and Public Key Encryptions	269
10.5 Key Management: Generation, Transportation, and Distribution	269
10.5.1 The Key Exchange Problem.....	270
10.5.2 Key Distribution Centers (KDCs)	271
10.5.3 Public Key Management	273
10.5.4 Key Escrow	276
10.6 Public Key Infrastructure (PKI).....	277
10.6.1 Certificates.....	277
10.6.2 Certificate Authority	278
10.6.3 Registration Authority (RA).....	278
10.6.4 Lightweight Directory Access Protocols (LDAP)	278
10.6.5 Role of Cryptography in Communication	278
10.7 Hash Function	279
10.8 Digital Signatures	280
10.9 References	282
10.10 Exercises	283
10.11 Advanced Exercises	283
11. Firewalls.....	285
11.1 Definition.....	285
11.2 Types of Firewalls	289
11.2.1 Packet Inspection Firewalls.....	289
11.2.2 Application Proxy Server: Filtering Based on Known Services.....	295
11.2.3 Virtual Private Network (VPN) Firewalls.....	300
11.2.4 Small Office or Home (SOHO) Firewalls.....	301
11.2.5 NAT Firewalls.....	302
11.3 Configuration and Implementation of a Firewall	302
11.4 The Demilitarized Zone (DMZ)	304
11.4.1 Scalability and Increasing Security in a DMZ	306
11.5 Improving Security Through the Firewall.....	307
11.6 Firewall Forensics	309
11.7 Firewall Services and Limitations	309
11.7.1 Firewall Services	310
11.7.2 Limitations of Firewalls	310
11.8 References	311
11.9 Exercises.....	312

11.10	Advanced Exercises	312
12.	System Intrusion Detection and Prevention	315
12.1	Definition	315
12.2	Intrusion Detection.....	316
12.2.1	The System Intrusion Process	316
12.2.2	The Dangers of System Intrusions	318
12.3	Intrusion Detection Systems (IDSs).....	319
12.3.1	Anomaly Detection.....	320
12.3.2	Misuse Detection.....	322
12.4	Types of Intrusion Detection Systems	323
12.4.1	Network-Based Intrusion Detection Systems (NIDSs).....	323
12.4.2	Host-Based Intrusion Detection Systems (HIDSs)	330
12.4.3	The Hybrid Intrusion Detection System.....	332
12.5	The Changing Nature of IDS Tools	333
12.6	Other Types of Intrusion Detection Systems	333
12.6.1	System Integrity Verifiers (SIVs).....	333
12.6.2	Log File Monitors (LFMs)	334
12.6.3	HoneyPots	334
12.7	Response to System Intrusion	336
12.7.1	Incident Response Team	336
12.7.2	IDS Logs as Evidence	337
12.8	Challenges to Intrusion Detection Systems	337
12.8.1	Deploying IDS in Switched Environments	338
12.9	Implementing an Intrusion Detection System.....	339
12.10	Intrusion Prevention Systems (IPS).....	339
12.10.1	Network-Based Intrusion Prevention Systems (NIPSs).....	340
12.10.2	Host-Based Intrusion Prevention Systems (HIPSs)	341
12.11	Intrusion Detection Tools	343
12.12	References.....	344
12.13	Exercises	345
12.14	Advanced Exercises	346
13.	Computer and Network Forensics	347
13.1	Definition.....	347
13.2	Computer Forensics	349
13.2.1	History of Computer Forensics	349
13.2.2	Elements of Computer Forensics	350
13.2.3	Investigative Procedures	352
13.2.4	Analysis of Evidence.....	360
13.3	Network Forensics	367
13.3.1	Intrusion Analysis	368

13.3.2	Damage Assessment.....	374
13.4	Forensics Tools.....	374
13.4.1	Computer Forensics Tools.....	375
13.4.2	Network Forensics Tools	381
13.5	References.....	383
13.6	Exercises	384
13.7	Advanced Exercises.....	384
14.	Virus and Content Filtering.....	387
14.1	Definition.....	387
14.2	Scanning, Filtering, and Blocking	387
14.2.1	Content Scanning	388
14.2.2	Inclusion Filtering	389
14.2.3	Exclusion Filtering	389
14.2.4	Other Types of Content Filtering	390
14.2.5	Location of Content Filters	391
14.3	Virus Filtering.....	393
14.3.1	Viruses.....	393
14.4	Content Filtering.....	402
14.4.1	Application Level Filtering	402
14.4.2	Packet Level Filtering and Blocking.....	404
14.4.3	Filtered Material.....	406
14.5	Spam	407
14.6	References.....	409
14.7	Exercises	410
14.8	Advanced Exercises.....	410
15.	Security Evaluations of Computer Products.....	411
15.1	Introduction.....	411
15.2	Security Standards and Criteria	412
15.3	The Product Security Evaluation Process.....	412
15.3.1	Purpose of Evaluation	413
15.3.2	Criteria.....	413
15.3.3	Process of Evaluation	414
15.3.4	Structure of Evaluation.....	415
15.3.5	Outcomes/Benefits	416
15.4	Computer Products Evaluation Standards	416
15.5	Major Evaluation Criteria.....	417
15.5.1	The Orange Book	417
15.5.2	U.S. Federal Criteria.....	420
15.5.3	Information Technology Security Evaluation Criteria (ITSEC).....	421

15.5.4	The Trusted Network Interpretation (TNI): The Red Book	421
15.5.5	Common Criteria (CC)	422
15.6	Does Evaluation Mean Security?	422
15.7	References	422
15.8	Exercises	423
15.9	Advanced Exercises	423
16.	Computer Network Security Protocols and Standards...	425
16.1	Introduction	425
16.2	Application Level Security	426
16.2.1	Pretty Good Privacy (PGP)	426
16.2.2	Secure/Multipurpose Internet Mail Extension (S/MIME) ...	429
16.2.3	Secure-HTTP (S-HTTP)	430
16.2.4	Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)	434
16.2.5	Secure Electronic Transactions (SET)	435
16.2.6	Kerberos	437
16.3	Security in the Transport Layer	440
16.3.1	Secure Socket Layer (SSL)	441
16.3.2	Transport Layer Security (TLS)	444
16.4	Security in the Network Layer	446
16.4.1	Internet Protocol Security (IPSec)	446
16.4.2	Virtual Private Networks (VPNs)	451
16.5	Security in the Link Layer and over LANS	456
16.5.1	Point-to-Point Protocol (PPP)	456
16.5.2	Remote Authentication Dial-In User Service (RADIUS) ...	457
16.5.3	Terminal Access Controller Access Control System (TACACS+)	459
16.6	References	460
16.7	Exercises	460
16.8	Advanced Exercises	461
17.	Security in Wireless Networks and Devices.....	463
17.1	Introduction	463
17.2	Cellular Wireless Communication Network Infrastructure	464
17.2.1	Development of Cellular Technology	467
17.2.2	Limited and Fixed Wireless Communication Networks	472
17.3	Wireless LAN (WLAN) or Wireless Fidelity (Wi-Fi)	474
17.3.1	WLAN (Wi-Fi) Technology	475
17.3.2	Mobile IP and Wireless Application Protocol (WAP)	475
17.4	Standards for Wireless Networks	478
17.4.1	The IEEE 802.11	480
17.4.2	Bluetooth	480

17.5 Security in Wireless Networks	482
17.5.1 WLANs Security Concerns	483
17.5.2 Best Practices for Wi-Fi Security Problems	489
17.5.3 Hope on the Horizon for WEP	491
17.6 References	491
17.7 Exercises	492
17.8 Advanced Exercises	493
18. Other Efforts to Secure Information and Computer Networks.....	495
18.1 Introduction.....	495
18.2 Legislation	496
18.3 Regulation.....	496
18.4 Self-Regulation	497
18.4.1 Hardware-Based Self-Regulation.....	497
18.4.2 Software-Based Self-Regulation	498
18.5 Education	499
18.5.1 Focused Education	500
18.5.2 Mass Education	500
18.6 Reporting Centers	501
18.7 Market Forces	502
18.8 Activism.....	502
18.8.1 Advocacy.....	502
18.8.2 Hotlines	503
18.9 References.....	503
18.10 Exercises	504
18.11 Advanced Exercises	505
19. Looking Ahead – Security Beyond Computer Networks	507
19.1 Introduction.....	507
19.2 Collective Security Initiatives and Best Practices	508
19.2.1 The U.S. National Strategy to Secure Cyberspace.....	508
19.2.2 Council of Europe Convention on Cyber Crime	509
19.3 References.....	510