

---

# *Contents*

<b>Preface</b> .....	xiii
<b>Acknowledgments</b> .....	xix
<b>The Author</b> .....	xxi
<b>Part I Introduction to Network Concepts and Threats</b> .....	1
<b>1 Network Architecture</b> .....	3
1.1 Layered Network Architecture .....	3
1.2 Overview of a Protocol .....	12
1.3 Layered Network Model .....	15
Homework Problems and Lab Experiments .....	20
References .....	21
<b>2 Network Protocols</b> .....	23
2.1 Protocol Specifications .....	23
2.2 Addresses .....	29
2.3 Headers .....	35
Homework Problems and Lab Experiments .....	37
References .....	37
<b>3 The Internet</b> .....	39
3.1 Addressing .....	41
3.1.1 Address Spoofing .....	45
3.1.2 IP Addresses .....	46
3.1.3 Host Name to IP Address Mapping .....	47
3.2 Client-Server Model .....	49
3.3 Routing .....	54
Homework Problems and Lab Experiments .....	57
References .....	59

<b>4</b>	<b>Taxonomy of Network-Based Vulnerabilities</b> .....	61
4.1	Network Security Threat Model .....	61
4.2	The Taxonomy .....	69
4.2.1	Header-Based Vulnerabilities and Attacks .....	69
4.2.2	Protocol-Based Vulnerabilities and Attacks .....	70
4.2.3	Authentication-Based Vulnerabilities and Attacks .....	73
4.2.4	Traffic-Based Vulnerabilities and Attacks .....	75
4.3	Applying the Taxonomy .....	76
	Homework Problems and Lab Experiments .....	78
	References .....	79
<b>Part II Lower-Layer Security</b> .....		<b>83</b>
<b>5</b>	<b>Physical Network Layer Overview</b> .....	<b>85</b>
5.1	Common Attack Methods .....	87
5.1.1	Hardware Address Spoofing .....	87
5.1.2	Network Sniffing .....	89
5.1.3	Physical Attacks .....	90
5.2	Wired Network Protocols .....	92
5.2.1	Ethernet Protocol .....	92
5.2.2	Header-Based Attacks .....	101
5.2.3	Protocol-Based Attacks .....	101
5.2.4	Authentication-Based Attacks .....	102
5.2.5	Traffic-Based Attacks .....	104
5.3	Wireless Network Protocols .....	106
5.3.1	Header-Based Attacks .....	114
5.3.2	Protocol-Based Attacks .....	114
5.3.3	Authentication-Based Attacks .....	116
5.3.4	Traffic-Based Attacks .....	119
5.4	Common Countermeasures .....	124
5.4.1	Virtual Local Area Networks (VLANs) .....	124
5.4.2	Network Access Control (NAC) .....	126
5.5	General Comments .....	128
	Homework Problems and Lab Experiments .....	129
	References .....	131

<b>Network Layer Protocols</b> .....	135
6.1 IP Version 4 Protocol .....	137
6.1.1 IP Addressing .....	138
6.1.2 Routing .....	143
6.1.3 Packet Format .....	149
6.1.4 Address Resolution Protocol (ARP) .....	153
6.1.5 Internet Control Messaging Protocol (ICMP) .....	156
6.1.5.1 ICMP Echo Request (TYPE = 8) and Reply (TYPE = 0) .....	157
6.1.5.2 ICMP Timestamp Request (TYPE = 13) and Reply (TYPE = 14) .....	158
6.1.5.3 ICMP Destination Unreachable (TYPE = 0) .....	158
6.1.5.4 ICMP Time Exceeded (TYPE = 11) .....	158
6.1.5.5 ICMP Redirection (TYPE = 5) .....	159
6.1.6 Putting It All Together .....	159
6.1.6.1 Scenario 1 (H1 to H2) .....	160
6.1.6.2 Scenario 2 (H1 to H3) .....	162
6.1.6.3 Scenario 3 (H1 to H4) .....	164
6.1.6.4 Scenario 4 (H1 to H5) .....	166
6.1.6.5 Scenario 5 (H1 to No Host on Network 1) .....	168
6.1.6.6 Scenario 6 (H1 to No Host on Network 2) .....	170
6.1.7 Header-Based Attacks .....	172
6.1.8 Protocol-Based Attacks .....	173
6.1.9 Authentication-Based Attacks .....	174
6.1.10 Traffic-Based Attacks .....	177
6.2 BOOTP and DHCP .....	181
6.2.1 BOOTP Protocol .....	182
6.2.2 DHCP Protocol .....	185
6.2.3 Header-Based Attacks .....	186
6.2.4 Protocol-Based Attacks .....	186
6.2.5 Authentication-Based Attacks .....	189
6.2.6 Traffic-Based Attacks .....	190
6.3 IP Version 6 Protocol .....	190
6.3.1 Packet Format .....	191
6.3.2 ICMP Version 6 Protocol .....	194

6.4	Common IP Layer Countermeasures .....	195
6.4.1	IP Filtering .....	195
6.4.2	Network Address Translation (NAT) .....	196
6.4.3	Virtual Private Network (VPN) .....	203
6.4.4	IPSEC .....	206
	Homework Problems and Lab Experiments .....	208
	References .....	215
<b>7</b>	<b>Transport Layer Protocols .....</b>	<b>221</b>
7.1	Transmission Control Protocol (TCP) .....	221
7.1.1	Multiplexing .....	221
7.1.2	Connection Management .....	223
7.1.3	Data Transfer .....	223
7.1.4	Special Services .....	224
7.1.5	Error Reporting .....	225
7.1.6	TCP Protocol .....	225
7.1.7	TCP Packet Format .....	228
7.1.8	Header-Based Attacks .....	229
7.1.9	Protocol-Based Attacks .....	230
7.1.10	Authentication-Based Attacks .....	237
7.1.11	Traffic-Based Attacks .....	237
7.2	User Datagram Protocol (UDP) .....	238
7.2.1	Packet Format .....	239
7.2.2	Header- and Protocol-Based Attacks .....	239
7.2.3	Authentication-Based Attacks .....	239
7.2.4	Traffic-Based Attacks .....	239
7.3	Domain Name Service (DNS) .....	239
7.3.1	DNS Protocol .....	242
7.3.2	DNS Packet Format .....	245
7.3.3	Header-Based Attacks .....	248
7.3.4	Protocol-Based Attacks .....	248
7.3.5	Authentication-Based Attacks .....	248
7.3.6	Traffic-Based Attacks .....	250
7.4	Common Countermeasures .....	251
7.4.1	Transport Layer Security (TLS) .....	251
	Homework Problems and Lab Experiments .....	253
	References .....	254

<b>Part III Application Layer Security</b> .....	259
<b>8 Application Layer Overview</b> .....	261
8.1 Sockets .....	263
8.2 Common Attack Methods .....	266
8.2.1 Header-Based Attacks .....	266
8.2.2 Protocol-Based Attacks .....	267
8.2.3 Authentication-Based Attacks .....	267
8.2.4 Traffic-Based Attacks .....	268
Homework Problems and Lab Experiments .....	268
References .....	270
<b>9 Email</b> .....	271
9.1 Simple Mail Transfer Protocol .....	274
9.1.1 Vulnerabilities, Attacks, and Countermeasures .....	278
9.1.1.1 Header-Based Attacks .....	278
9.1.1.2 Protocol-Based Attacks .....	278
9.1.1.3 Authentication-Based Attacks .....	278
9.1.1.4 Traffic-Based Attacks .....	282
9.1.1.5 General Countermeasures .....	282
9.2 POP and IMAP .....	283
9.2.1 Vulnerabilities, Attacks, and Countermeasures .....	288
9.2.1.1 Header- and Protocol-Based Attacks .....	288
9.2.1.2 Authentication-Based Attacks .....	288
9.2.1.3 Traffic-Based Attacks .....	290
9.3 MIME .....	290
9.3.1 Vulnerabilities, Attacks, and Countermeasures .....	297
9.3.1.1 Header-Based Attacks .....	298
9.3.1.2 Protocol-Based Attacks .....	298
9.3.1.3 Authentication-Based Attacks .....	299
9.3.1.4 Traffic-Based Attacks .....	299
9.4 General Email Countermeasures .....	300
9.4.1 Encryption and Authentication .....	300
9.4.2 Email Filtering .....	304
9.4.3 Content Filtering .....	308
9.4.4 Email Forensics .....	309
Homework Problems and Lab Experiments .....	314
References .....	317

<b>10</b>	<b>Web Security</b> .....	321
10.1	Hypertext Transfer Protocol (HTTP).....	324
10.1.1	Command Message .....	324
10.1.2	Response Message .....	326
10.1.3	HTTP Headers .....	326
10.1.4	Vulnerabilities, Attacks, and Countermeasures .....	333
10.1.4.1	Header-Based Attacks .....	333
10.1.4.2	Protocol-Based Attacks .....	334
10.1.4.3	Authentication-Based Attacks .....	334
10.1.4.4	Traffic-Based Attacks .....	336
10.2	Hypertext Markup Language (HTML) .....	340
10.2.1	Vulnerabilities, Attacks, and Countermeasures .....	343
10.2.1.1	Header-Based Attacks .....	343
10.2.1.2	Protocol-Based Attacks .....	344
10.2.1.3	Authentication-Based Attacks .....	344
10.2.1.4	Traffic-Based Attacks .....	344
10.3	Server-Side Security .....	345
10.3.1	Vulnerabilities, Attacks, and Countermeasures .....	347
10.3.1.1	Header-Based Attacks .....	347
10.3.1.2	Protocol-Based Attacks .....	348
10.3.1.3	Authentication-Based Attacks .....	348
10.3.1.4	Traffic-Based Attacks .....	348
10.4	Client-Side Security .....	349
10.4.1	Vulnerabilities, Attacks, and Countermeasures .....	351
10.4.1.1	Header- and Protocol-Based Attacks .....	351
10.4.1.2	Authentication-Based Attacks .....	351
10.4.1.3	Traffic-Based Attacks .....	352
10.5	General Web Countermeasures .....	352
10.5.1	URL Filtering .....	353
10.5.2	Content Filtering .....	356
	Homework Problems and Lab Experiments .....	359
	References .....	361
<b>11</b>	<b>Remote Access Security</b> .....	367
11.1	Terminal-Based Remote Access (TELNET, rlogin, and X-Windows) .....	368
11.1.1	TELNET .....	368
11.1.2	rlogin .....	372

11.1.3	X-Windows .....	376
11.1.4	Vulnerabilities, Attacks, and Countermeasures .....	378
11.1.4.1	Header-Based Attacks .....	379
11.1.4.2	Protocol-Based Attacks .....	379
11.1.4.3	Authentication-Based Attacks.....	379
11.1.4.4	Traffic-Based Attacks .....	381
11.2	File Transfer Protocols .....	382
11.2.1	File Transfer Protocol (FTP) .....	382
11.2.2	Trivial FTP.....	389
11.2.3	RCP.....	390
11.2.4	Vulnerabilities, Attacks, and Countermeasures .....	391
11.2.4.1	Header-Based Attacks .....	391
11.2.4.2	Protocol-Based Attacks .....	391
11.2.4.3	Authentication-Based Attacks.....	392
11.2.4.4	Traffic-Based Attacks .....	393
11.3	Peer-to-Peer Networks .....	394
11.3.1	Centralized Peer to Peer .....	396
11.3.2	KaZaA .....	399
11.3.3	Decentralized Peer to Peer .....	400
11.3.3.1	Limewire, Bearshare, and Gnutella .....	401
11.3.4	Vulnerabilities, Attacks, and Countermeasures .....	403
11.3.4.1	Header- and Protocol-Based Attacks.....	403
11.3.4.2	Authentication-Based Attacks.....	403
11.3.4.3	Traffic-Based Attacks .....	404
11.3.4.4	Peer-to-Peer Countermeasures .....	404
11.4	General Countermeasures .....	406
11.4.1	Encrypted Remote Access .....	406
11.4.2	SSH.....	407
11.4.3	Remote Desktop .....	410
11.4.4	Secure File Transfer (SFTP, FTPS, HTTPS) .....	411
	Homework Problems and Lab Experiments .....	412
	References.....	415
<b>Part IV</b>	<b>Network-Based Mitigation .....</b>	<b>425</b>
<b>12</b>	<b>Common Network Security Devices .....</b>	<b>427</b>
12.1	Network Firewalls .....	427
12.2	Network-Based Intrusion Detection and Prevention .....	433
12.3	Network-Based Data Loss Prevention.....	437

Homework Problems and Lab Experiments .....	439
References .....	440
<b>Appendix A Cryptology .....</b>	<b>445</b>
<b>Appendix B Laboratory Configuration .....</b>	<b>455</b>
<b>Appendix C Homework Solutions .....</b>	<b>461</b>
<b>Index .....</b>	<b>473</b>