

contents

Preface xv

Acknowledgements xvii

Chapter 1 Introduction to Wireless LANs 1

1.1	SECURING THE INSECURE	2
1.1.1	AAE AND A FUNCTIONS	2
1.1.2	AUTHENTICATION	2
1.1.3	AUTHORIZATION	3
1.1.4	ENCRYPTION	3
1.1.5	ACCOUNTING	4
1.1.6	PRACTICAL NETWORK PROTECTION METHODS	4
1.2	NETWORK ARCHITECTURE	7
1.2.1	BASIC NETWORKING DEVICES	7
1.2.2	THE WIRELESS LAN STATION	8
1.2.3	THE ACCESS POINT	10
1.2.4	THE WIRELESS BRIDGE	13
1.2.5	THE WIRELESS ROUTER	13
1.2.6	THE BASIC SERVICE SET	18
1.2.7	THE EXTENDED SERVICE SET (ESS)	20
1.2.8	STATION SERVICES	21
1.3	IEEE WIRELESS LAN STANDARDS	27
1.3.1	THE BASIC IEEE 802.11 STANDARD	28
1.3.2	802.11B	30
1.3.3	802.11A	30
1.3.4	802.11C	30
1.3.5	802.11D	31
1.3.6	802.11E	31
1.3.7	802.11F	31

1.3.8	802.11G	31
1.3.9	802.11H	31
1.3.10	802.11I	32
1.4	BOOK PREVIEW	32
1.4.1	FRAME FORMATS AND BASIC SECURITY OPERATIONS	32
1.4.2	UNDERSTANDING WIRELESS SIGNALS	33
1.4.3	UNDERSTANDING WEP	33
1.4.4	SECURITY RISKS	33
1.4.5	PROPRIETARY SECURITY ENHANCEMENT TECHNIQUES	33
1.4.6	STANDARDS BASED SECURITY	34

Chapter 2 Frame Formats and Basic Security Operation 35

2.1	FRAME FORMATS	35
2.1.1	BASIC FRAME FORMAT	36
2.1.2	FRAME CONTROL FIELD	36
2.1.3	CONTROL FRAMES	43
2.1.4	MANAGEMENT FRAMES	46
2.1.5	THE AUTHENTICATION PROCESS	53
2.2	WEP AND PRIVACY	53
2.2.1	MISCONCEPTIONS	53
2.2.2	DEVELOPMENT CONSTRAINTS	54
2.2.3	DEFICIENCIES	58

Chapter 3 Understanding Wireless Signals 61

3.1	THE WIRELESS RF SPECTRUM AND BASIC MEASUREMENTS	62
3.1.1	FREQUENCY	62
3.1.2	PERIOD AND WAVELENGTH	63
3.1.3	BANDWIDTH	64
3.1.4	THE FREQUENCY SPECTRUM	64
3.1.5	POWER MEASUREMENTS	66
3.1.6	POWER LEVEL	69
3.1.7	SIGNAL-TO-NOISE RATIO	69
3.2	ANTENNA BASICS	71
3.2.1	BASIC OPERATION	72
3.2.2	CATEGORIES	73
3.2.3	ANTENNA GAIN	73

3.2.4	DIRECTIONALITY AND EIRP	74
3.2.5	POWER LEVELS	74
3.2.6	PROPAGATION LOSS	75
3.2.7	INCREASING ANTENNA GAIN	76
3.2.8	POWER LIMITS	77
3.2.9	RECEIVER SENSITIVITY	78
3.2.10	REDUCING EMITTED RADIATION	79
3.2.11	HORIZONTAL TRANSMISSION DISTANCE	80
3.2.12	EQUIPMENT POSITIONING	81
3.2.13	USING MONITORING EQUIPMENT	83

Chapter 4 Understanding WEP 85

4.1	THE WEP FRAME BODY	86
4.1.1	THE IV	86
4.1.2	THE ICV	87
4.1.3	THE NAKED DEFAULT	87
4.1.4	WEP KEY LIMITATIONS	90
4.2	LOCATING AND OBSERVING WIRELESS LAN TRAFFIC	91
4.2.1	NETWORK STUMBLER	91
4.2.2	MONITORING WITH AIROPEEK	93
4.3	RC4	97
4.3.1	OVERVIEW	97
4.3.2	OPERATION	98
4.3.3	ILLUSTRATIVE EXAMPLE	99
4.3.4	STRENGTHS AND WEAKNESSES	102
4.4	WEP WEAKNESS	102
4.4.1	UNSAFE AT ANY SIZE	102
4.4.2	THE INSECURITY OF 802.11	103
4.4.3	EXPLOITING RC4 WEAKNESS	107
4.4.4	BREAKING WEP	108
4.4.5	AIRSNORT	109
4.4.6	WEP CRACK	110

Chapter 5 Security Risks and Countermeasures 113

5.1	THE SSID	113
5.1.1	OVERVIEW	114
5.1.2	OVERRIDING THE SSID	114

5.1.3	OBTAINING THE SSID	115
5.1.4	COUNTERMEASURES	117
5.2	EAVESDROPPING	117
5.2.1	OVERVIEW	117
5.2.2	THREATS	118
5.2.3	COUNTERMEASURES	118
5.3	MASQUERADE	121
5.3.1	OVERVIEW	121
5.3.2	COUNTERMEASURES	122
5.4	DATA MODIFICATION	124
5.4.1	OVERVIEW	124
5.4.2	COUNTERMEASURES	124
5.5	FILE SHARING	124
5.5.1	OVERVIEW	124
5.5.2	WINDOWS 95	125
5.5.3	WINDOWS 2000	128
5.5.4	COUNTERMEASURES	131
5.6	JAMMING	131
5.6.1	OVERVIEW	131
5.6.2	COUNTERMEASURES	132
5.7	ENCRYPTION ATTACKS	133
5.7.1	OVERVIEW	134
5.7.2	COUNTERMEASURES	135
5.8	SNMP	135
5.8.1	CODING FLAWS	136
5.8.2	SNMP VERSIONS	136
5.8.3	COUNTERMEASURES	141
5.9	BROADCAST MONITORING	141
5.9.1	OVERVIEW	142
5.9.2	COUNTERMEASURES	144
5.10	ACCESSING A MANAGEMENT CONSOLE	145
5.10.1	OVERVIEW	145
5.10.2	COUNTERMEASURES	145
5.11	THEFT OF HARDWARE	146
5.11.1	OVERVIEW	146
5.11.2	COUNTERMEASURES	146
5.12	ROGUE ACCESS POINTS	147
5.12.1	OVERVIEW	147
5.12.2	COUNTERMEASURES	147

Chapter 6 Proprietary Security Enhancement Techniques 149

6.1	MAC ADDRESS AUTHENTICATION	150
6.1.1	IEEE 802.11 AUTHENTICATION	150
6.1.2	IMPLEMENTATION METHODS	151
6.1.3	ACCESS POINT UTILIZATION	151
6.1.4	USING A RADIUS SERVER	151
6.1.5	DATAFLOW	151
6.1.6	LIMITATIONS WHEN USING AN AP	151
6.1.7	LIMITATIONS USING A RADIUS SERVER	152
6.1.8	CHAP	153
6.1.9	VISITOR CONSIDERATIONS	154
6.2	CLOSED SYSTEM OPTION	154
6.2.1	OVERVIEW	155
6.2.2	LIMITATIONS	155
6.3	SYSTEM ACCESS PASS PHRASE	155
6.3.1	OVERVIEW	155
6.3.2	NETWORK ACCESS	156
6.3.3	LIMITATIONS	156
6.4	DYNAMIC KEY EXCHANGE AND WEAK KEY AVOIDANCE	156
6.4.1	DYNAMIC KEY EXCHANGE	157
6.4.2	OVERVIEW	157
6.4.3	LIMITATIONS	157
6.4.4	WEAK KEY AVOIDANCE	158
6.4.5	OVERVIEW	158
6.4.6	LIMITATIONS	158
6.5	PROTECTING WIRELESS CLIENTS FROM THE PUBLIC NETWORK	158
6.5.1	OVERVIEW	159
6.5.2	CISCO ACCESS LISTS	159
6.5.3	SMC NETWORKS BARRICADE PACKET FILTERING	161
6.5.4	LIMITATIONS	163
6.5.5	SUMMARY	165
6.6	ANTENNA ORIENTATION AND SHIELDING	166
6.6.1	OVERVIEW	166
6.6.2	ALTERING SIGNAL STRENGTH	166
6.6.3	LIMITATIONS	167
6.7	MINIMIZING TRANSMIT POWER AND ANTENNA CONTROL	168
6.7.1	POWER MANAGEMENT	168
6.7.2	ANTENNA CONTROL	170

6.7.3	POWER LEVEL CONTROL	170
6.7.4	LIMITATIONS	171
6.8	WIRELESS INTRUSION DETECTION	172
6.8.1	OVERVIEW	172
6.8.2	LIMITATIONS	172
6.9	LEAP	173
6.9.1	OVERVIEW	173
6.9.2	OPERATION	174
6.9.3	CONFIGURATION	174
6.9.4	CONFIGURING THE ACCESS POINT	175
6.9.5	CLIENT CONFIGURATION	175
6.9.6	ENABLING WEP	177
6.9.7	LIMITATIONS	181

Chapter 7 Standards Based Security 183

7.1	THE IEEE 802.1X STANDARD	183
7.1.1	OVERVIEW	183
7.1.2	GENERAL OPERATION	184
7.1.3	DATA FLOW	185
7.1.4	THE EAP PROTOCOL	187
7.1.5	MESSAGE TYPES	188
7.1.6	EAP PACKET FORMAT	188
7.1.7	THE DUAL-PORT AUTHENTICATION MODEL	189
7.1.8	SECURITY LIMITATIONS	189
7.1.9	USING THE CISCO AIRONET 350	193
7.1.10	CLIENT SETUP	193
7.1.11	NETWORK SECURITY	198
7.1.12	USING WINDOWS XP	200
7.1.13	ACCESS POINT SETUP	203
7.1.14	SECURITY SETUP	209
7.1.15	ACCESS	209
7.1.16	SECURITY SETUP OPTIONS	211
7.1.17	CLOSING THOUGHTS	219
7.2	EVOLVING ENCRYPTION	220
7.2.1	TKIP	221
7.2.2	AES	222

7.3	VPNS AND TUNNELING PROTOCOLS	224
7.3.1	VPN OVERVIEW	224
7.3.2	NEED FOR SECURITY	225
7.3.3	TYPES OF VPNS	226
7.3.4	APPLICABILITY TO WIRELESS LANS	228
7.3.5	VPN PROTOCOLS	229
7.3.6	PPTP	229
7.3.7	L2TP AND IPSec	232
7.3.8	VPN OPERATIONS	234

Appendix A Wireless LAN Security Checklist 245

Index 249