

[For more information about this title, click here.](#)

CONTENTS

Preface	xvii
Chapter 1 Introduction to Wireless LAN Security Standards	1
Wireless Defined	2
Factors of Security	2
Theft	3
Access Control	4
Authentication	4
Encryption	5
Safeguards	6
Intrusion Detection Systems	7
IEEE	9
WECA	9
Wi-Fi	9
The Many Flavors of 802.11	9
FHSS	10
DSSS	11
OFDM	12
Bluetooth	12
Differences between the Wireless Standards	13
Conclusion: How Security Applies	14
Chapter 2 Technology	17
Comparisons	17
HomeRF	18
802.11 versus SWAP	18

SWAP Specification	19
Integrating Wireless Phone and Data	19
Bluetooth	19
Wireless Hacking	20
NetStumbler	20
NetStumbler Software Uses	22
Script Kiddies	22
Facts	24
Bluetooth Technology	25
Bluetooth Background	25
What Gives Bluetooth Its Bite?	26
Bluetooth Spectrum Hopping	27
Bluetooth Connections	28
Enforcing Security	30
Link Me Up!	31
Conclusion: The Future of the WLAN	32
Chapter 3 Wireless LAN Security Factors	33
Enabling Encryption Security	35
WEP Encryption	36
Encrypting 802.11b?	36
Network Interface Cards	36
Cross-Platform Hacking	37
Eavesdropping	39
Breaking In!	40
Counterfeiting	40
Wireless DoS Attack	41
Points of Vulnerability	42
Your Best Defense Against an Attack	45
Conclusion: Keeping Your WLAN Secure	47
Chapter 4 Issues in Wireless Security	49
The State of Wireless LAN Security	50
Securing Your WLAN	50
Authenticating Data	51
Client Authentication in a Closed System	53
Shared Key Authentication	53
RC4	53
Ensuring Privacy	54
Keeping Data Intact	55

Managing Keys	56
WLAN Vulnerabilities	58
Subtle Attacks	59
Common Security Pitfalls	59
Poor Security, Better than No Security at All!	59
Short Keys	59
Initialization Vectors	60
Shared Keys	60
Checks and Balances for Packets	60
Authentication	61
Location! Location! Location!	61
Attack Patterns	62
Active Attack Patterns	62
Passive Attacks	63
Conclusion	63
Chapter 5 The 802.11 Standard Defined	65
The 802.11 Standard	66
Issues to Consider	66
Expanding the Network Standard	69
Ad Hoc Networks	69
Extended Service Set	69
Wireless Radio Standard	70
The Standard Algorithm	71
Address Spaces	72
The 802.11 Standard in Security	72
Encryption	73
Timing and Power Management	73
Speed	75
Compatibility	75
Standard “Flavors” of 802.11	76
802.11a	76
802.11b	77
802.11d	77
802.11e	78
802.11f	78
802.11g	78
802.11h	79
802.11i	79
Conclusion: Evolution of the 802.11 Standard	80

Chapter 6	802.11 Security Infrastructure	83
	Point-to-Point Wireless Application Security	84
	Point of Interception	84
	Wireless Vulnerability	86
	Building a Private Wireless Infrastructure	88
	Vulnerable Encryption	89
	Commercial Security Infrastructure	89
	Building a Private Infrastructure	90
	Items to Compromise	91
	Deploying Your Wireless Infrastructure	92
	Determining Requirements	92
	Choosing a Flavor of 802.11	93
	Security Design	96
	Monitoring Activity	97
	Conclusion: Maintaining a Secure Infrastructure	97
Chapter 7	802.11 Encryption: Wired Equivalent	99
	Privacy	99
	Why WEP?	100
	Defending Your Systems	100
	WEP Mechanics	103
	Wireless Security Encryption	103
	Insecure Keys	104
	Taking a Performance Hit	104
	Wireless Authentication	105
	Known WEP Imperfections	107
	Access Control	108
	IRL Security	109
	Points of Vulnerability	109
	Conclusion: Finding Security in an Unsecured World	111
Chapter 8	Unauthorized Access and Privacy	113
	Privacy in Jeopardy	114
	Passive Attacks	114
	Broadcast Monitoring	115
	Active Attacks	116
	The “Evil” Access Point	117
	Data Privacy	117
	Compromising Privacy in Public Places	118
	Protecting Your Privacy	118

Public or Private?	120
Safer Computing	120
The “Human” Factor	122
Defining the Bullet Points in a Security Policy	122
Training	124
Physical Security	124
Wireless Range	126
Conclusion: Common Sense Access Controls	127
Chapter 9 Open System Authentication	131
What is Open System Authentication?	132
802.11 Networks on Windows XP	133
User Administration	134
Managing Keys in an Open System	135
Authentication Concerns	135
802.11b Security Algorithms	136
Authentication Support	137
Shared-key Authentication	138
Secret Keys	138
The WEP Algorithm	138
Static Vulnerabilities	139
NIC Security	139
Wireless NIC Power Settings	140
Open System to WEP Authentication	141
Port-based Network Access Control	141
Securely Identifying Wireless Traffic	143
Extensible Authentication Protocol	144
Conclusion: Open System versus Closed System Authentication	146
Chapter 10 Direct Sequence Spread Spectrum	147
802.11 DSSS	148
Standardization	148
MAC Layers	149
CSMA	150
Roaming	150
Power Requirements	151
Increasing Data Transmission	151
FHSS Security	154
Hop Sequences	155

FHSS versus DSSS	155
Frequency Allocation	156
Open System Security	158
It's All About...Timing	159
System Roaming	160
Conclusion: Spectrum Safety!	160
Chapter 11 Wi-Fi Equipment Issues	163
Issues in Wi-Fi Deployment	164
Wireless Equipment Vendors	164
WLAN Equipment Considerations	165
Equipment Vendors	167
Market Trends	168
Technology Issues	169
Access Point-centric Configuration	170
Mobile Device Configuration	170
Building Extensions to Access Points	171
Directional Broadcasting	172
Cost Concerns	172
The Costs of Effective Security	174
Wired versus Wireless Security	176
Vendor Trials	176
Conclusion: Next-generation Wireless Equipment	178
Chapter 12 Cross-Platform Wireless User Security	181
WLAN Assignment Applications	182
Cost Concerns	182
Macintosh WLANs	183
Lindows OS	185
Orinoco Wireless	185
Handheld Devices	186
Cross-platform Wireless Security Concerns	187
Initialization Vector Collisions	188
Key Reuse	188
Evil Packets	189
Real-time Decryption	189
802.11 Security Issues	189
Windows XP Wireless Connectivity	192
Windows XP WEP Authentication	192
Windows XP Wireless Functionality	194

WLAN NIC Vendors	194
Conclusion: All Vendors Must Get Along!	195
Chapter 13 Security Breach Vulnerabilities	197
Intercepting Wireless Network Traffic	198
Wireless 802.11b	199
Proximity Attack	199
Securing Your Network	201
WAP Attack!	201
Encryption	201
Commonsense Measures	203
PnP Networked Devices	203
Windows Users	204
Macintosh Computers	205
Linux Boxes	205
Hacking the Network Printer	206
Printer Servers	207
Defending Against Attacks	208
Conclusion: Limiting Your Vulnerabilities	211
Chapter 14 Access Control Schemes	215
Authentication	216
Windows XP Access and Authentication Schemes	217
Access Control Procedures	217
Physical Security	218
Controlling Access to Access Points	219
Physical Access Point Security	220
Secure Access Point Management Issues	221
Preventive Measures	225
MAC the Knife	225
VPN	225
IP Addressing Issues	227
Conclusion: Ensuring “Secure” Access Control	229
Chapter 15 Wireless Laptop Users (PC and Mac)	231
Laptop Physical Security	232
Protection	232
Hardware Solutions	233
Public Key Infrastructure	237
Portable Biometrics	237

Reducing WEP Vulnerabilities	239
Securing the WLAN	241
Platform Bias	241
Wireless Laptop Network Support	242
Enhancing Mobile Security	243
Remote Users	243
Conclusion: Evolving Laptop Security	244
Chapter 16 Administrative Security	247
Authentication Solutions	248
Passwords	249
Building the Firewall	249
Intrusion Detection Systems	250
Host-based IDS	252
Network-based IDS	253
Host IDS versus Network IDS	253
Why Have an IDS?	253
The Computer as the Decision Maker	254
Real Live People	255
Security Vulnerability Assessment	256
Risk Assessment	257
Conclusion: Best Defense Is a Good Offense!	260
Chapter 17 Security Issues for Wireless Applications (Wireless PDAs)	263
Protecting Information	264
PDA Data	264
Seeking Security	265
Security Functionality	266
Access Control	266
HotSync	266
Infrared	266
Building an Effective Mobile Security Policy	268
Protecting Mobile Resources	268
Wireless Connectivity	268
HotSync Security	270
Infrared Authentication	270
Establishing a Security Policy	271
Privacy Concerns	272
Why PDAs Require Privacy	272

Maintaining Access Control	273
Data Encryption	273
SecurID	273
Intranet Access with Your PDA	274
How Hackers Fit into the Equation	275
Security Concerns	275
PDAs as Diagnostic Tools	275
PocketDOS	276
Wireless Service Providers	277
GoAmerica Communications	277
SprintPCS	277
AT&T Wireless IP Network	278
Conclusion: Mobile Wireless Computing	279
Chapter 18 The Future of Wi-Fi Security?	281
Privacy Regulations	282
Patriot Act, 2001 (USPA)	282
Graham-Leach-Bliley (GLB) Act, 2001	282
Fair Credit Reporting Act, 1970, 1996 (FCRA)	282
Children's Online Privacy Protection Act of 1998 (COPPA)	283
Health Insurance Portability and Accountability Act (HIPPA) [August 21, 1996]	283
Pervasive Computing	283
Wireless Mobile Computing	284
Evolving Security	284
Basic Encryption	285
WEP	285
Protecting Access	285
Denial of Service Attacks	286
Evolving Standards	286
Competing Standards	287
Enhancing Your Wireless Security	289
Biometrics	290
Assessing WLAN Strengths and Weaknesses	290
Combining Future WLAN Technology	291
Smart Systems	292
Scrambled Data	292
OS Platform Evolution	292
Windows XP Security	293
Macintosh OS X	294

Palm and PocketPC	294
Linux	294
Windows OS	295
Preventing Network Intrusion Attempts	295
Network Servers	296
File Servers	296
Printer Servers	297
Conclusion: The Future of Wireless Networking	297
Index	299