

# Contents

Foreword . . . . .	.xxi
Introduction . . . . .	.xxiii
<b>Part I Introduction to Wireless Hacking . . . . .</b>	<b>.1</b>
<b>Chapter 1 A Brief Overview of the Wireless World . . . . .</b>	<b>.3</b>
Introduction to Wi-Fi . . . . .	.4
The History and Basics of 802.11 . . . . .	.4
IEEE Alphabet Soup . . . . .	.5
802.11b . . . . .	.5
802.11a . . . . .	.7
802.11g . . . . .	.9
Ad-Hoc and Infrastructure Modes . . . . .	.9
Connecting to an Access Point . . . . .	.10
FCC Regulations . . . . .	.14
FCC and IEEE Regulations . . . . .	.14
Why Wi-Fi? . . . . .	.15
Benefits for Property Owners . . . . .	.16
Benefits for Volunteers . . . . .	.16
Social Ramifications . . . . .	.17
Security in a Community Wireless Network . . . . .	.18
Every Computer Needs to Be Protected . . . . .	.18
Legal Liability . . . . .	.19
Defending the Neighborhood . . . . .	.20
Summary . . . . .	.20
<b>Chapter 2 SoCalFreeNet.org: Building Large Scale Community Wireless Networks . . . . .</b>	<b>.23</b>
Introduction . . . . .	.24
Wireless Distribution System (WDS) . . . . .	.24
5 GHz Links . . . . .	.25
Working with Client Devices . . . . .	.26
Competing with the Phone/Cable Companies . . . . .	.28

Outfitting Coffee Shops and Retail Locations	.29
Getting the Neighborhood Involved	.30
Summary	.31
<b>Chapter 3 Securing Our Wireless Community</b>	<b>.33</b>
Introduction	.34
The Captive Portal	.35
Preparing for the Hack	.35
Wiring the Network for Security	.36
Choosing the Captive Portal Software and Hardware	.37
Performing the Hack: Enabling Our Captive Portal	.40
Writing Our Terms of Service	.41
Captive Portal Graphics	.42
Building a PPTP VPN	.44
Preparing for the Hack	.45
Performing the Hack: Enabling the VPN	.45
Configuring Our Community Users	.50
Hacking the Mind of a Wireless User	.54
Preparing for the Hack	.54
Performing the Hack: The Beginning and the End	.54
Other Hacks	.56
<b>Part II Hacking Projects</b>	<b>.57</b>
<b>Chapter 4 Wireless Access Points</b>	<b>.59</b>
Introduction	.60
Wi-Fi Meets Linux	.60
Reflashing	.60
Linksys WRT54g	.60
Sveasoft	.61
NewBroadcom	.69
HyperWRT	.70
eWRT	.71
Wifi-box	.72
Batbox	.74
OpenWRT	.75
WRT54G Shortcomings	.75
Soekris Single-Board Computers	.75
net4501	.76

net4511	.77
net4521	.78
net4526	.79
net4801	.79
Soekris Accessories	.80
Proxim 8571 802.11a Access Point	.81
Preparing for the Hack	.83
Performing the Hack	.84
Under the Hood: How the Hack Works	.89
Summary	.95
<b>Chapter 5 Wireless Client Access Devices</b>	<b>.97</b>
Introduction	.98
Notebook Computers	.98
PCMCIA Cards	.98
Mini-PCI Cards	.99
Desktop Computers	.100
PCI Cards	.101
USB Devices	.101
Ethernet Bridges	.103
PDAs	.103
Compact Flash	.104
Secure Digital IO Cards	.105
WarDriving	.105
Why Are People WarDriving?	.106
Preparing for the Hack	.106
Required Equipment	.107
WarDriving Software	.107
Optional Equipment	.108
WarDriving Ethics	.112
Other Resources	.113
<b>Part III Software Projects</b>	<b>.115</b>
<b>Chapter 6 Wireless Operating Systems</b>	<b>.117</b>
Introduction	.118
m0n0wall—Powerful, Elegant, Simple	.120
Preparing for the Hack	.121

m0n0wall on a Standard PC . . . . .	121
m0n0wall on a Single Board Computer (SBC) . . . . .	121
Performing the Hack . . . . .	122
Downloading a Recent Version . . . . .	123
Creating a CD-ROM from Windows . . . . .	123
Creating a Compact Flash (CF) Card from Windows . . . . .	125
Starting Your Standard PC . . . . .	127
Starting Your SBC . . . . .	131
Configuring m0n0wall . . . . .	134
Under the Hood: How the Hack Works . . . . .	148
Pebble—Powerful, Raw, Complete . . . . .	148
Preparing for the Hack . . . . .	149
Performing the Hack . . . . .	150
Creating a Boot CD and Starting Knoppix . . . . .	150
Configuring the Compact Flash Reader/Writer . . . . .	152
Formatting the Compact Flash Card . . . . .	154
Downloading Pebble . . . . .	156
Copying Pebble to the Compact Flash . . . . .	156
Booting Pebble . . . . .	158
Configuring Pebble . . . . .	158
Under the Hood: How the Hack Works . . . . .	160
<b>Chapter 7 Monitoring Your Network . . . . .</b>	<b>163</b>
Introduction . . . . .	164
Enabling SNMP . . . . .	165
Preparing for the Hack . . . . .	165
Performing the Hack . . . . .	165
Under the Hood: How the Hack Works . . . . .	167
Getif and SNMP Exploration for Microsoft Windows . . . . .	168
Preparing for the Hack . . . . .	168
Performing the Hack . . . . .	168
Retrieving Device Interface Information . . . . .	169
Exploring the SNMP OIDs . . . . .	170
Graphing the Data . . . . .	172
Under the Hood: How the Hack Works . . . . .	173
STG and SNMP Graphs for Microsoft Windows . . . . .	173
Preparing for the Hack . . . . .	174

Performing the Hack . . . . .	174
Under the Hood: How the Hack Works . . . . .	177
Cacti and Comprehensive Network Graphs . . . . .	177
Preparing for the Hack . . . . .	178
Apache . . . . .	178
PHP . . . . .	179
Perl . . . . .	179
RRDTool . . . . .	179
MySQL . . . . .	179
Cacti . . . . .	179
Performing the Hack . . . . .	179
Installing Apache . . . . .	180
Installing PHP . . . . .	182
Installing Perl . . . . .	185
Installing RRDTool . . . . .	185
Installing MySQL . . . . .	186
Miscellaneous Settings . . . . .	186
Installing Cactid and Cacti . . . . .	187
Graphing Data in Cacti . . . . .	192
Under the Hood: How the Hack Works . . . . .	197
Additional References . . . . .	198
<b>Chapter 8 Low-Cost Commercial Options . . . . .</b>	<b>199</b>
Introduction . . . . .	200
Sputnik . . . . .	200
Sputnik Access Points . . . . .	200
Sputnik Control Center . . . . .	202
Sputnik Features . . . . .	204
Captive Portal . . . . .	204
Pre-Paid Module . . . . .	205
A Sputnik Revolution . . . . .	207
Sveasoft . . . . .	207
MikroTik . . . . .	209
Summary . . . . .	212

<b>Chapter 9 Mesh Networking</b>	<b>.215</b>
Introduction	.216
Preparing the Hacks	.217
The Basic Definitions	.218
WDS (Wireless Distribution System)	.220
Real World Example	.222
Example Two: LocustWorld Mesh Networks	.222
Summary	.223
Additional Resources on the Web	.224
<b>Part IV Antennas and Outdoor Enclosure Projects</b>	<b>.225</b>
<b>Chapter 10 Antennas</b>	<b>.227</b>
Introduction	.228
Before You Start: Basic Concepts and Definitions	.228
Federal Communications Commission	.234
Attenuation in Cables, Connectors, and Materials	.236
System Grounding and Lightning Protection	.238
Building a Coffee Can Antenna	.240
Preparing for the Hack	.240
Performing the Hack	.241
Under the Hood: How the Hack Works	.243
Troubleshooting Common Antenna Issues	.244
The Future of Antennas	.244
Summary	.245
<b>Chapter 11 Building Outdoor Enclosures and Antenna Masts</b>	<b>.247</b>
Introduction	.248
Building Outdoor Enclosures	.248
Preparing for the Hack	.249
Selecting a Raw Enclosure	.249
Hardware Selection	.252
Performing the Hack	.255
Metal NEMA 3 Enclosures	.255
Under the Hood: How the Hack Works	.263
Building Antenna Masts	.263
Preparing for the Hack	.264

Performing the Hack . . . . .	.265
The Free-Standing Antenna Mast . . . . .	.265
Direct Mount Antenna Masts . . . . .	.269
Lightning Protection . . . . .	.272
Summary . . . . .	.273
<b>Chapter 12 Solar-Powered Access Points and Repeaters . . . . .</b>	<b>.275</b>
Introduction . . . . .	.276
Preparing for the Hack . . . . .	.276
Calculating Power Requirements . . . . .	.276
Battery Selection . . . . .	.279
Selecting a Solar Panel . . . . .	.281
Performing the Hack . . . . .	.286
Structure . . . . .	.286
Solar Panel . . . . .	.288
Electrical . . . . .	.288
Electronics . . . . .	.294
Under the Hood: How the Hack Works . . . . .	.295
The Batteries . . . . .	.296
The Solar Panel . . . . .	.296
<b>Appendix A Wireless 802.11 Hacks . . . . .</b>	<b>.299</b>
Introduction . . . . .	.300
Wireless NIC/PCMCIA Card Modifications: Adding an	
External Antenna Connector . . . . .	.301
Preparing for the Hack . . . . .	.302
Performing the Hack . . . . .	.303
Removing the Cover . . . . .	.303
Moving the Capacitor . . . . .	.305
Attaching the New Connector . . . . .	.307
Under the Hood: How the Hack Works . . . . .	.308
OpenAP (Instant802): Reprogramming Your Access Point	
with Linux . . . . .	.308
Preparing for the Hack . . . . .	.309
Performing the Hack . . . . .	.310
Installing the SRAM Card . . . . .	.311
Power Me Up, Scotty! . . . . .	.314

Under the Hood: How the Hack Works . . . . .	.314
Having Fun with the Dell 1184 Access Point . . . . .	.314
Preparing for the Hack . . . . .	.315
Performing the Hack . . . . .	.316
Under the Hood: How the Hack Works . . . . .	.321
Summary . . . . .	.321
Additional Resources and Other Hacks . . . . .	.321
User Groups . . . . .	.321
Research and Articles . . . . .	.322
Products and Tools . . . . .	.322
<b>Index . . . . .</b>	<b>.325</b>