WIRELESS HACKS

Tips & Tools for Building, Extending, and Securing Your Network

Rob Flickenger & Roger Weeks
With a new foreword by Glenn Fleishman
WIRELESS HACKS

Tips & Tools for Building, Extending, and Securing Your Network

Wireless networks are being deployed around the world and making ubiquitous connectivity more the rule than the exception—providing service (often free) to millions of users who suddenly need nothing more than a laptop and wireless card to get online. But getting online is only half the battle; getting the most out of wireless networking hardware and software remains far from obvious.

Completely revised and expanded—with over 35 brand-new hacks, just as many hacks completely overhauled, and the rest meticulously updated—this new edition of Wireless Hacks brings you the knowledge of experts who apply what they know in the real world every day. Whether you're running Windows, Linux, or Mac OS X, you'll find practical techniques for extending range, increasing throughput, managing wireless resources, and generally making your wireless networking vision a reality. Learn how to:

- Use Bluetooth, mobile radios, mobile data networks, cellular phones, Wi-Fi hotspots, GPS, and other exotic methods to keep you connected anywhere
- Make wireless devices do things the designers didn’t intend and turn wired devices into wireless ones
- Employ practical methods for detecting, analyzing, and monitoring your own wireless networks and those available to the public
- Extend the range of your network, making the best possible use of the available radio spectrum
- Design and build your own wireless access points and antennas
- Survey and engineer long-distance network links spanning several miles
- Understand the security issues of wireless networking, and protect yourself and your users from unauthorized access and eavesdropping

Whether your wireless network needs to extend to the other edge of your office, throughout your large house, or to the other end of town, this collection of nonobvious, “from the field” techniques will show you how to get the job done.

Got a Hack? Go to: hacks.oreilly.com

WIRELESS HACKS
Other resources from O'Reilly

**Related titles**
- VoIP Hacks™
- Network Security Hacks™
- Windows XP Hacks™
- Nokia Smartphone Hacks™
- Palm and Treo Hacks™
- Blackberry Hacks™
- Skype Hacks™
- Building Wireless Community Networks
- Windows XP Unwired
- Linux Unwired
- 802.11 Wireless
- Networks: The Definitive Guide

**Hacks Series Home**

*hacks.oreilly.com* is a community site for developers and power users of all stripes. Readers learn from each other as they share their favorite tips and tools for Mac OS X, Linux, Google, Windows XP, and more.

**oreilly.com**

*oreilly.com* is more than a complete catalog of O’Reilly books. You’ll also find links to news, events, articles, weblogs, sample chapters, and code examples.

**oreillynet.com**

*oreillynet.com* is the essential portal for developers interested in open and emerging technologies, including new platforms, programming languages, and operating systems.

**Conferences**

O’Reilly brings diverse innovators together to nurture the ideas that spark revolutionary industries. We specialize in documenting the latest tools and systems, translating the innovator’s knowledge into useful skills for those in the trenches. Visit *conferences.oreilly.com* for our upcoming events.

Safari Books Online (*safaribooksonline.com*) is the premier online reference library for programmers and IT professionals. Conduct searches across more than 1,000 books. Subscribers can zero in on answers to time-critical questions in a matter of seconds. Read the books on your Bookshelf from cover to cover or simply flip to the page you need. Try it today for free.
SECOND EDITION

WIRELESS HACKS

Rob Flickenger and Roger Weeks
Contents

Foreword ................................................................. ix
Credits ................................................................. xi
Preface ................................................................. xvii

Chapter 1. Bluetooth, Mobile Phones, and GPS ......................... 1
  1. Set Up Bluetooth on Linux .................................. 1
  2. Set Up Bluetooth on Windows XP ......................... 4
  3. Connect Mac OS X with a Bluetooth Phone ............... 10
  4. Connect Linux with a Bluetooth Phone ................... 15
  5. Connect Windows XP with a Bluetooth Phone .......... 21
  6. Use Your Treo as a Modem .................................. 23
  7. Send SMS from a PowerBook ............................... 28
  8. Remote Control Mac OS X with Bluetooth Phones and PDAs 31
  9. Remote Control Linux with a Bluetooth Phone ......... 35
 10. Control XMMS with Bluetooth ............................. 37
 11. Liven Up Parties with a Participatory Slideshow ....... 39
 12. Send SMS from Linux ......................................... 42
 13. Remote Control Windows with Bluetooth Phones and PDAs 44
 14. Control Your Bluetooth Phone with FMA ............... 49
 15. Control Your Computer from Your Palm .................. 55
 16. Control Your Home Theater from Your Palm ............ 62
 17. Choose a Cellular Data Plan ............................... 67
 18. Blog from Your Mobile Phone .............................. 73
 19. Get Google Maps on Your Mobile Phone ................ 81
20. Share Your GPS  82
21. Broadcast Your GPS Position  85
22. Map Wi-Fi Networks with Kismet and GPSd  89

Chapter 2. Network Discovery and Monitoring  92
23. Find All Available Wireless Networks  92
24. Discover Networks with NetStumbler  100
25. Detect Networks with Handheld PCs  105
26. Find and Join Wireless Networks with AP Radar  110
27. Detect Networks on Mac OS X  113
28. Scan Passively with KisMAC  116
29. Detect Networks with Kismet  119
30. Monitor Wireless Links in Linux with Wavemon  125
31. Analyze Traffic with Ethereal  127
32. Track 802.11 Frames in Ethereal  130
33. Watch Network Traffic  132
34. grep Your Network  134
35. Check Wi-Fi Network Performance with Qcheck  137
36. Estimate Network Performance  140
37. Get Real-Time Network Stats  142
38. Graph Your Wireless Performance  144
39. Find Radio Manufacturers by MAC  148

Chapter 3. Wireless Security  151
40. Stop Moochers from Stealing Your Wi-Fi Bandwidth  152
41. Visualize a Network  156
42. Secure Your Linux Network with WPA  159
43. Control Wireless Access by MAC  167
44. Authenticate Wireless Users  172
45. Forward Ports over SSH  178
46. Proxy Web Traffic over SSH  179
47. Securely Connect Two Networks  181
48. Generate a Tunnel Configuration Automatically  186
49. Poll Wireless Clients  191
50. Interrogate the Network  192
51. Track Wireless Users  194
### Chapter 4. Hardware Hacks

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>Add an External Antenna</td>
<td>197</td>
</tr>
<tr>
<td>53</td>
<td>Do-It-Yourself Access Point Hardware</td>
<td>199</td>
</tr>
<tr>
<td>54</td>
<td>Boot from a Compact Flash Hard Drive</td>
<td>204</td>
</tr>
<tr>
<td>55</td>
<td>Increase the Range of a PowerBook</td>
<td>206</td>
</tr>
<tr>
<td>56</td>
<td>Send Power over Your Ethernet</td>
<td>207</td>
</tr>
<tr>
<td>57</td>
<td>The NoCat Night Light</td>
<td>211</td>
</tr>
<tr>
<td>58</td>
<td>Upgrade the Linksys WET11</td>
<td>214</td>
</tr>
<tr>
<td>59</td>
<td>Scan for Wireless Networks Automatically</td>
<td>217</td>
</tr>
<tr>
<td>60</td>
<td>Backlight Your Zipit</td>
<td>223</td>
</tr>
<tr>
<td>61</td>
<td>Unwire Your Pistol Mouse</td>
<td>231</td>
</tr>
<tr>
<td>62</td>
<td>Mobilize Your WRT54G with the WiFiCar</td>
<td>241</td>
</tr>
</tbody>
</table>

### Chapter 5. Software Hacks

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>Build Your Own Access Point with Linux</td>
<td>253</td>
</tr>
<tr>
<td>64</td>
<td>Bridge Your Linux AP</td>
<td>261</td>
</tr>
<tr>
<td>65</td>
<td>Protect Your Bridge with a Firewall</td>
<td>263</td>
</tr>
<tr>
<td>66</td>
<td>Filter MAC with HostAP and Madwifi</td>
<td>264</td>
</tr>
<tr>
<td>67</td>
<td>Upgrade Your Wireless Router</td>
<td>266</td>
</tr>
<tr>
<td>68</td>
<td>Set Up an OLSR Mesh Network</td>
<td>271</td>
</tr>
<tr>
<td>69</td>
<td>Extend Your Wireless Network with WDS</td>
<td>275</td>
</tr>
<tr>
<td>70</td>
<td>Pebble</td>
<td>280</td>
</tr>
<tr>
<td>71</td>
<td>Wall Off Your Wireless</td>
<td>282</td>
</tr>
<tr>
<td>72</td>
<td>Run Your Mac as an Access Point</td>
<td>289</td>
</tr>
<tr>
<td>73</td>
<td>Run Linux on the Zipit Wireless Messenger</td>
<td>291</td>
</tr>
<tr>
<td>74</td>
<td>Capture Wireless Users with NoCatAuth</td>
<td>297</td>
</tr>
<tr>
<td>75</td>
<td>Capture Wireless Users on a Small Scale</td>
<td>301</td>
</tr>
<tr>
<td>76</td>
<td>Build an Online Community in Your Offline Neighborhood</td>
<td>302</td>
</tr>
<tr>
<td>77</td>
<td>Manage Multiple AirPort Base Stations</td>
<td>308</td>
</tr>
<tr>
<td>78</td>
<td>Advertise Bonjour Services in Linux</td>
<td>312</td>
</tr>
<tr>
<td>79</td>
<td>Advertise Any Service with Bonjour in Mac OS X</td>
<td>316</td>
</tr>
<tr>
<td>80</td>
<td>Redirect “Brought to you by” Bonjour Ads</td>
<td>317</td>
</tr>
<tr>
<td>81</td>
<td>Use a Windows-Based Wireless Card in Linux</td>
<td>319</td>
</tr>
<tr>
<td>82</td>
<td>Use Your Orinoco Card with Hermes AP</td>
<td>323</td>
</tr>
</tbody>
</table>
It’s a pleasure to watch a book mature. The first edition of *Wireless Hacks* gave me a warm feeling inside, like holding my hands over the vacuum tube in a pre-transistor radio. The glow of this book illuminated Rob Flickenger’s intense interest in spreading knowledge of cool stuff in order to spread more knowledge about the world in general.

This second edition, which brings the practical deployer (building networks is part of his day job) and fellow wireless hacker Roger Weeks onboard, feels more like a device constructed by the love child of The Professor from *Gilligan’s Island* and Mr. Spock: it beeps, it twitters, there are coconut shreds, and then, surprisingly, it produces a glass of tea out of thin air or transports several people to geosynchronous orbit.

The book has grown up, just a little, which makes it no less charming or useful. *Wireless Hacks* isn’t about breaking technology to serve your needs. Rather, it’s about bending it. So much of today’s wireless networking hardware, software, and firmware has been carefully tailored to suit what the manufacturer or service provider feels you are entitled to do with it. But we own the tech and, for unlicensed networks, we own the airwaves. *Wireless Hacks* stands up, raises its hand, and says, “Excuse me, I don’t buy into your world view.”

A great number of the tips and some of the lengthy hacks in the book should become standard operating procedure at companies that use wireless tech and want to increase its value for their use. Being able to more broadly use Bluetooth beyond limited, support purposes; extending range of equipment legally without using expensive proprietary or identically branded devices; or having the flexibility to hack open the hardware or software to fiddle with its innards and do what one wants is less about hacking and more about just making things work.
Wireless Hacks could as easily have been titled It’s My Equipment, Damnit, and perhaps those of you reading the foreword to find out whether this book is for you would find that title more comforting. While I was raised with a soldering iron in one hand and a diode in the other, self-modding my 1979-era OSI CIP 6502-based computer, I guarantee that while the spirit pervades this book, molten metal isn’t a necessity—but it is an option—for carrying out most of the tasks in the book.

Rob and Roger and their legion of colleagues contributing tips are trying to make the world smaller by extending signals further. This book is another step in the right direction for a small, wireless world.

—Glenn Fleishman
August 28, 2005, Seattle, WA
About the Authors

Rob Flickenger has been a professional systems administrator for more than ten years, and an all-around hacker for as long as he can remember. Rob enjoys spreading the good word of open networks, open standards, and ubiquitous wireless networking. His current professional project is Metrix Communication LLC, which provides wireless hardware and software that embodies the same open source principles he rants about in his books. Rob also works with the U.N. and various international organizations to bring these ideas to places where communications infrastructure is badly needed. He hopes that all of this effort is contributing toward the ultimate goal of infinite bandwidth everywhere for free. He is the author of two other O’Reilly books: *Linux Server Hacks* and *Building Wireless Community Networks*, which is now in its second edition.

Roger Weeks has over a decade of experience in systems and network administration. He’s been building Linux systems at home and in the enterprise since 1998, and recommends that you check out http://freenetworks.org if you’re interested in community wireless. He is currently the senior network administrator for Mendocino Community Network, a small ISP in coastal northern California. MCN is owned by the local school district, and puts their profits back into the local schools. Roger is a coauthor of another O’Reilly book, *Linux Unwired*.

Contributors

The following people contributed code, hacks, writing, and inspiration to this book:

- Richard Baguley is a freelance journalist who writes about computers, technology, and video for publications such as *PC World*, *Wired*, and...
camcorderinfo.com. He lives in the San Francisco Bay area with his wife Kath and a French Bulldog called Fester. His home is shared with an ever-changing variety of foster cats who like nothing better than to gnaw on any cables that he leaves lying around, which explains why he likes wireless networking so much.

• Marcel Bilal is a computer scientist, with a focus on Wireless LAN technologies. He lives in Berlin, Germany and works for an IT-service provider (IT-Dienstleistungszentrum Berlin) as a systems admin. You can find him at http://aws.netzfund.de or marcel_bilal@web.de.

• James Duncan Davidson is a freelance author, software developer, and consultant focusing on Mac OS X and related technologies. He is the author of Running Mac OS X Panther, coauthor (with Rael Dornfest) of Mac OS X Panther Hacks, coauthor (with Apple Computer, Inc) of Learning Cocoa with Objective-C, and coauthor (with Michael Beam) of Cocoa in a Nutshell, all published by O’Reilly Media. Duncan is also a contributor to the O’Reilly Network (http://www.oreillynet.com), as well as publisher of his own web site, x180 (http://x180.net/). In what sometimes seems like a previous life, Duncan created the widely used Apache Tomcat and Apache Ant and was instrumental in their donation to the Apache Software Foundation by Sun Microsystems. He was also the specification lead and author of two versions of the Java Servlet API and two versions of the Java API for XML Processing (JAXP).

• Schuyler Erle (http://nocat.net) hacks on free software and agitates for the cause of community networking. Schuyler is also chief architect of NoCatAuth, a leading open source captive portal application.


• Preston Gralla is the author of more than 30 books about computers and the Internet, including Windows XP Hacks, Internet Annoyances, and Windows XP Power Hound. He’s been writing about technology since the dawn of the PC, was a founding editor of both PC Week and PC/Computing, an executive editor of ZDNet and CNet, and has contributed to dozens of publications, including PC Magazine, The Los Angeles Times, USA Today, and Computerworld, among others.

• Bryan Hurley studies Computer Science at the University of Maryland, Baltimore County. He is working on wearable computing research dealing with location, audio, and mood sensing. In addition to cutting the cord on the PistolMouse, he has built augmented reality systems at the United States Naval Research Laboratory in Washington, D.C. He lives in Columbia, Maryland. Bryan can be contacted at hurleymail@gmail.com.
• Jeff Ishaq (http://www.ishaq.biz) is a software engineer and writer living in Santa Cruz, California. He is the author of Treo Fan Book for O'Reilly, and has been developing Palm software since 1996. In his spare time, he enjoys eating spicy food, trail running, playing guitar, and alpine snowboarding. He hopes someday to organize his office.

• Brian Jepson is an O'Reilly editor, programmer, and coauthor of Mac OS X Tiger for Unix Geeks and Linux Unwired. He's also a volunteer systems administrator and all-around geek for AS220 (http://www.as220.org), a nonprofit arts center in Providence, Rhode Island. AS220 gives Rhode Island artists uncensored and unjuried forums for their work. These forums include galleries, performance space, and publications. Brian sees to it that technology, especially free software, supports that mission.

• Scott MacHaffie (http://www.nonvi.com/sm) is a programmer. He learned to program in 1980 and has been getting paid for it since 1987. He has a B.S. and an M.S. in Computer Science, from University of Washington and Portland State University, respectively. He has studied Human-Computer Interactions and User Interface design for many years. Scott writes games for Palm OS devices as a hobby. He and his wife are learning to speak Irish Gaelic. Scott also teaches aikido when he can get a break from his twin boys, and he is knowledgeable about early Celtic, Irish, and Scottish history.

• Dr. Trevor Marshall (http://www.trevormarshall.com), based in the heart of Southern California’s “Digital Coast,” offers a full spectrum of consulting services in technologies ranging from Wi-Fi security and Internet infrastructure through RF, hardware, software, and audio/video to biomedical and prepress. Previous speaking engagements have included COMDEX, Microprocessor Forums, and WLAN/Wi-Fi Security conferences in Paris, Boston, and Santa Clara.

• Damon McCormick is a recent University of California, Berkeley, graduate with degrees in Electrical Engineering, Computer Science, and Philosophy. He enjoys the contradiction between an area of study that actively seeks an implementation of strong artificial intelligence and an area of study that claims strong artificial intelligence is practically impossible. Damon admits to computer security research and billiards addictions, and splits his spare time evenly between those activities and working on PlaceSite.

• Yasha Okshtein is an Interdisciplinary Engineering major at The Cooper Union for the Advancement of Science and Art. In his spare time, he tinkers with anything he can get his hands on, including Linux, RC
Cars, and various wireless devices. His web site is at http://yasha. okshtein.net and he can be reached at flyashi@gmail.com.

- Sean Savage is Project PlaceSite’s Founder and Chief Instigator. Sean coined the term zombie effect, which describes feelings of alienation that occur when people in a semipublic place like a cafe or pub tune out the people and activities around them as they focus on laptops, mobile phones, or televisions. The zombie effect, and possibilities for countering it, is a driving force behind Project PlaceSite. Sean also coined the term flash mob, which is now listed in the Oxford English Dictionary and first appeared on his web site (http://cheesebikini.com). In 2005 Sean graduated with a Masters degree from U.C. Berkeley’s School of Information Management & Systems. For two years he studied and designed location-based technology at Berkeley and, during the summer of 2004, at Intel Research Seattle. Sean is also a writer whose work has appeared in Wired, The Washington Post, The Miami Herald, and The Chicago Tribune.

- Terry Schmidt (http://www.nycwireless.net) is a leading expert on wireless networking technologies and applications. He has presented at major information technology conferences, including MacWorld, the O’Reilly Emerging Technologies Conference, and 802.11Planet.

- Cloyce D. Spradling is a full-time sysadmin and full-time developer of benchmarks and benchmark tools for one of SPEC’s (http://www.spec. org) member companies. He likes monkeys, pirates, watching cartoons, and traveling with his wife and their rubber chicken. He can be reached at cloyce+oreilly@headgear.org.

- Jo Walsh is a freelance hacker and software artist who started out building web systems for the Guardian, the ICA, and state51 in London. Jo is trying to combine her interests in maps, spatial annotation on the semantic web, Wi-Fi geolocation, public transport planning, open geodata, and bots into something resembling coherence: http://wirelesslondon.info, a localized wireless captive portal service.

- Matt Westervelt is the founder of SeattleWireless (http://seattlewireless. net) and an evangelist for FreeNetworks worldwide. He left the corporate world to start Metrix Communication LLC, a company created to supply FreeNetworkers with high quality, standards-based wireless networking products. As a child, he watched a lot of Sesame Street, and has a firm (perhaps misguided) belief that cooperation can solve a lot of the world’s problems.
• Ron Wickersham (http://www.alembic.com) is an inventor and the Chief Engineer at Alembic, Inc. where he designs guitar electronics. His hobbies involve everything interesting in the Universe including The Amateur Sky Survey and watering the flowers.

• Haihao Wu grew up in Shanghai and lives with his wife in Austin, Texas. He works for Freescale Semiconductor.

• Michael Juntao Yuan (http://www.MichaelYuan.com) is a mobile alpha geek and author of three mobile-technology–related books. Over the last couple of years, he has managed to accumulate more than a dozen smartphones; most of them are Nokia phones. He is the lead developer of Nokia’s Series 40 Java Blueprint Application and is actively involved in various standards committees helping to define the next-generation Java platform on mobile phones. Michael currently works for JBoss Inc., the Professional Open Source software company, focusing on next-generation Java enterprise middleware. Michael has a Ph.D. from the University of Texas at Austin. When he is not working, writing, or playing with gadgets, he likes to travel and take pictures. Check out his picture albums at http://www.jjcafe.net/photography.

Acknowledgments

This book is really a cooperative venture, regardless of the two names on the cover. As Rob said when the second edition was proposed, writing a Hacks book is not only writing, but also project management.

Thanks to all of our contributors who provided such great and new material for the book, and to our editor, Brian Sawyer, who has been a great resource throughout the whole process.

Rob

I’d like to thank my family and friends for their continuing support by giving me the encouragement (and occasionally, solitude) needed to complete my various little projects.

Many hacks in this book were inspired by conversations with countless hackers who willingly share their ideas with anyone who will listen. A few came from the weekly “hack night” sessions that SeattleWireless hosts to foster such cross-pollination of ideas. Without the free and enthusiastic exchange of ideas, this book would not have been possible. Thank you to all of the brilliant hackers around the planet who know that the value of sharing one’s ideas can greatly exceed the value of keeping an idea to oneself.
Edd Dumbill, Casey Halverson, and Richard Lotz all provided technical review for the book. Ken Caruso and Matt Westervelt provided equipment, ideas, and valuable insight. Thank you, gentlemen!

And thanks everyone at O’Reilly who made this book a reality, and who continue to help relieve information pain in the world.

Roger

I wouldn’t have dived deeply into things wireless if I hadn’t met Rob at one of the early NoCat meetings he held at O’Reilly back in 2001. The next couple of years were full of long-distance network building, late-night hacking, and a real sense of community, not only for me but for everyone who was involved in actually building a community wireless network. I can’t thank Rob enough.

I would also be amiss if I didn’t thank personally all of the “Cats”: Nate Boblitt, Adam Flaherty, Jim Rosenbaum, and Schuyler Erle. There isn’t anything that can’t get fixed, broken, and fixed even better when these guys are in the room.

During the entire time we’ve been married, my wife, Cynthia, has been totally understanding of the life of a geek. She puts up with long technical conversations, motherboards and computer pieces littering the floor, and even the long hours that come with working a network admin job. I love her more than words can express.
Preface

Wireless networking technology has shown an explosive growth worldwide over the past few years, bucking the general downward economic trend in the telecommunications industry. What is it about wireless networking that makes it so alluring on a grand scale? Why are there more than 75 million Wi-Fi devices worldwide, with some people projecting double that number by 2008? While marketing folks might tell you that the particular feature set and brand name of their product is driving demand, we believe the answer is much simpler: it’s magic.

Right where you are sitting now, there could be dozens of wireless data networks slinging information to the far corners of the Earth. A neighbor orders food online while someone across the street is using voice chat to talk to relatives (for free!) in Hong Kong, all the while someone upstairs is downloading a new album from their favorite band’s web site in San Francisco. The information flows all around you (and, indeed, even through you) without you seeing or hearing a thing. Make no mistake: wireless networking is probably the second most magical technology on the planet—just behind the Internet.

In hundreds of cities around the world, wireless networks are making ubiquitous connectivity more the rule than the exception, providing service (often free) to millions of users who suddenly need nothing more than a laptop and wireless card to get online. Wireless networking is getting people connected to each other more cheaply and easily than any other networking technology since the telephone.

Why Wireless Hacks?

The term hacking has a bad reputation in the popular press, where it is used to refer to someone who breaks into systems or wreaks havoc using computers as their weapon. Among enthusiasts, on the other hand, the term hack
refers to a “quick-and-dirty” solution to a problem, or to a clever way to get something done. The term hacker is taken very much as a compliment, referring to someone as being creative, and having the technical chops to get things done. O’Reilly’s Hacks series is an attempt to reclaim the word, document the ways people are hacking (in a good way), and pass the hacker ethic of creative participation on to the uninitiated. Seeing how others approach systems and problems is often the quickest way to learn about a new technology.

Wireless Hacks is about getting the most out of your wireless networking hardware and software. In this book, you will find practical techniques for extending range, increasing throughput, managing wireless resources, and generally making your wireless networking vision a reality. Remember that reality is what you can get away with, and wireless hackers have found that they can get away with quite a lot using surprisingly little. This book will show you some of the best bits of their collected experience.

How to Use This Book

You can read this book from cover to cover if you like, but for the most part, each hack stands on its own. So feel free to browse, flipping around to whatever sections interest you most.

How This Book Is Organized

This book is divided into several subjects by chapter:

Chapter 1, Bluetooth, Mobile Phones, and GPS

The last couple years have brought hundreds of millions of tiny battery-powered wireless devices to market. Some will get you an Internet connection just about anywhere with mobile phone service, while others keep your devices connected to the “last 10 feet,” and some cover the whole globe. This chapter demonstrates some uses for these technologies, which will keep your devices (and yourself) connected, without wires.

Chapter 2, Network Discovery and Monitoring

Wireless networking can be a lot of fun, but when it breaks, troubleshooting can be difficult without a good idea of what is really happening. This chapter will give you the tools you need to detect the presence of wireless networks, coordinate spectrum usage to avoid interference, and visualize network performance. It also covers a number of advanced data-monitoring techniques to pinpoint networking issues and even get an idea of your users’ online habits.
Chapter 3, *Wireless Security*

There has been a lot of press over the last few years about the insecurity of wireless networks. In many cases, these alarmist reports are in fact absolutely true: the vast majority of wireless networks are either unintentionally left open, or worse, use unreliable security methods. This chapter explores the current standards for securing wireless networks and suggests several strong methods for protecting yourself and your wireless users from abuse.

Chapter 4, *Hardware Hacks*

If it weren’t for the hardware, there would be no such thing as wireless networks. This extensive chapter tells you how to push wireless hardware to the limits, extending range and increasing performance and efficiency. It presents a large collection of components, along with sources and recommendations on how best to use them.

Chapter 5, *Software Hacks*

There also would be no such thing as wireless networks without the software, which ranges from the firmware that powers wireless cards and routers to the drivers required for those cards, up to general-purpose operating systems that can be used to build your own wireless access point, router, and firewall. This chapter covers all these topics and more.

Chapter 6, *Do-It-Yourself Antennas*

Since the first electrical spark was transmitted a few feet across a room more than 100 years ago, antenna design has been a fascination for wireless experimenters everywhere. This chapter presents several home-brew designs for wireless networking made by contributors from all over the world. These are practical, tested designs that can significantly extend the range of your wireless network.

Chapter 7, *Wireless Network Design*

Having the equipment in place is one thing, but being able to make a wireless segment stretch for miles requires real-world experience. This chapter is a collection of techniques to help simplify the job of building wireless networks that cover the area you require.

Appendix A, *Wireless Standards*

Wireless technology has not only produced impressive improvements to communications, but it has also produced an impressive list of acronyms. What is the difference between GPRS and GMRS? Which is fastest: 802.11, 802.11a, 802.11b, 802.11g, or 802.16? Exactly how do WiFi and Bluetooth fit into all of this? This appendix will give you a good idea of what problems each technology is designed to solve, their relative strengths and weaknesses, and how to make the best possible use of each to fulfill your communication needs.
Appendix B, Wireless Hardware Guide

Do you know the difference between a RP-TNC and a Reverse SMA connector? What about LMR versus Heliax antenna cabling? How do omni and sector antenna patterns differ, and why would you use one over the other? This appendix answers all of these questions and provides a comprehensive list of wireless equipment retailers.

Conventions Used in This Book

The following is a list of the typographical conventions used in this book:

*Italic*
Used to indicate new terms, URLs, filenames, file extensions, directories, and to highlight comments in examples. For example, a path in the filesystem will appear as `/usr/local`. Also used for lowercased names of programs and tools, such as `tcpdump`.

*Constant width*
Used to show code examples, the contents of files, packages, modules, directives, commands, and the output from commands.

*Constant width bold*
Used in examples and tables to show commands or other text that should be typed literally.

*Constant width italic*
Used in examples and tables to show text that should be replaced with user-supplied values.

*Gray type*
Used to indicate a cross-reference within the text.

\A backslash (\) at the end of a line of code is used to denote an unnatural line break; that is, you should not enter these as two lines of code, but as one continuous line. Multiple lines are used in these cases due to page width constraints.

*Menu symbols*
When looking at the menus for any application, you will see some symbols associated with keyboard shortcuts for a particular command. For example, to open a file, you would go to the File menu and select Open... (File → Open...).

You should pay special attention to notes set apart from the text with the following icons:
This is a tip, suggestion, or general note. It contains useful supplementary information about the topic at hand.

This is a warning or note of caution.

The thermometer icons, found next to each hack, indicate the relative complexity of the hack:

- beginner
- moderate
- expert

Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You do not need to contact us for permission unless you’re reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O’Reilly books does require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product’s documentation does require permission.


If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at permissions@oreilly.com.

How to Contact Us

We have tested and verified the information in this book to the best of our ability, but you may find that features have changed (or even that we have made mistakes!). As a reader of this book, you can help us to improve future editions by sending us your feedback. Please let us know about any errors, inaccuracies, bugs, missing ideas, unclear statements, and typos that you find anywhere in this book.
WRT
   getting meshed, 271
   uploading new firmware, 271
WRT54G, 200, 266
   mounting on Wi-Fi controllable car, 241–252
wvdial utility, 19

X
X11
   image viewers for slideshow, 40
   network image grabber, 157
   screensaver functions, turning off, 41
XMMS, controlling with Bluetooth, 37–38

Y
yagi antennas, 415
yum utility
   installing Bluetooth packages, 2
   installing Howl, 314

Z
Zaurus handheld, using Kismet, 109
Zero Configuration Networking, 312
zflash, 294, 295
Zipit Wireless Communicator,
   backlighting, 223–229
   EL panel driver board, 230
   getting it open, 224
   opening the LCD, 225
   preparing and installing EL panel, 227
   removing LCD reflector, 226
   removing mainboard, 225
   wiring, 228
Zipit Wireless Messenger
   running Linux, 291–297
   flashing Zipit, 292–293
Zipit Wireless Yahoo Group, 294
Colophon

Our look is the result of reader comments, our own experimentation, and feedback from distribution channels. Distinctive covers complement our distinctive approach to technical topics, breathing personality and life into potentially dry subjects.

The tool on the cover of Wireless Hacks is a wire cutter/pliers combo tool. It is typically used to cut or trim a piece of wire, and can bend it into an appropriate shape. In a pinch, it can also strip the insulation from heavy gauge wire, although a wire stripper is really the proper tool for that job. Its insulated handle provides a small measure of protection from electricity, but when using a wire cutter, be sure to first disconnect power from the wire you are cutting. Always wear eye protection when using a cutting device of any kind.

Philip Dangler was the production editor and proofreader for Wireless Hacks. Derek Di Matteo was the proofreader. Mary Brady and Colleen Gorman provided quality control. Ellen Troutman-Zaig wrote the index.

Ellie Volckhausen designed the cover of this book, based on a series design by Edie Freedman. The cover image is a photograph from the Stockbyte WorkTools CD. Linda Palo and Karen Montgomery produced the cover layout with QuarkXPress 4.1 using Adobe’s Helvetica Neue and ITC Galamb fonts.

David Futato designed the interior layout. This book was converted by Keith Fahlgren to FrameMaker 5.5.6 with a format conversion tool created by Erik Ray, Jason McIntosh, Neil Walls, and Mike Sierra that uses Perl and XML technologies. The text font is Linotype Birka; the heading font is Adobe Helvetica Neue Condensed; and the code font is LucasFont’s TheSans Mono Condensed. The illustrations that appear in the book were produced by Robert Romano and Jessamyn Read using Macromedia FreeHand MX and Adobe Photoshop CS. This colophon was written by Rob Flickenger.