SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

SYNGRESS
4
FREE
E-BOOKLETS
PUBLISHING

Linksys WRT54G

Ultimate Hacking

"A ROSETTA STONE FOR THE WRT54G"

- Never-Before-Seen and Documented Hacks, Including Wireless Spectrum Analysis
- Comprehensive Coverage of WRT54G Advanced Features
- Includes WRT54G Fun Projects and Tips for Hardware Hacking

Paul Asadoorian
Larry Pesce
Raúl Siles **Technical Editor**

VISIT US AT

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

This Page Intentionally Left Blank

SYNGRESS®

Linksys® WRT54G Ultimate Hacking

Paul Asadoorian
Larry Pesce
Raúl Siles Technical Editor

Elsevier, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Elsevier, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	**SERIAL NUMBER**
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	GHJ923HJMN
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Linksys WRT54G Ultimate Hacking

Copyright © 2007 by Elsevier, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 978-1-59749-166-2

Publisher: Amorette Pedersen
Acquisitions Editor: Andrew Williams
Technical Editor: Raúl Siles
Cover Designer: Michael Kavish

Project Manager: Jay Donahue
Page Layout and Art: Patricia Lupien
Copy Editor: Audrey Doyle
Indexer: Michael Ferreira

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Acknowledgments and Dedications

Paul Asadoorian

Dedicated to my wife Shannon and mother Paula who stuck by me and supported me throughout the entire project, and to my grandfather who always said,“You get out of something what you put into it.”

Larry Pesce

Dedicated to my wife Kristin and my mother Pam, who stand by me to pick up the slack when I put too many irons in the fire, and for all of their support and encouragement.

Thank you!

Paul and Larry would like to collectively thank the following for their support, inspiration, hard work and encouragement in the concept and execution of this book: Mike Baker, Andrew Williams, Raúl Siles,The OpenWrt developers, Mike Kershaw,Jay Beale, Renderman, Andrew Lockhart, members of irc.freenode.net #pauldotcom, #openwrt, everyone who contributed to the OpenWrt Wiki, Rocco, Victor,Joshua Wright, David Cook, anyone else we forgot to mention, and everyone who has ever hacked a WRT54G and put information about it on the Internet.

Book Web Site

For updates, new tutorials, and all new things related to WRT54G hacking by the authors, please visit www.wrt54ghacks.com.

This Page Intentionally Left Blank

Co-authors

Paul Asadoorian (GCIA, GCIH) is the Lead IT Security Engineer for a large University in the New England area. In the past 6 years he has been responsible for intrusion detection, firewalls, VPN, and networking assessments/penetration testing in the educational IT space. He speaks frequently on topics such as wireless security at various events, such as the MIT Security Camp. Paul's research has been featured in numerous publications such as *Network Intrusion Detection, 3rd Edition*, Securityfocus.com, and the SANS Reading Room. In addition to owning and operating an independent security consulting company, Defensive Intuition, Paul is also the host of PaulDotCom Security Weekly (http://pauldotcom.com), a weekly podcast discussing IT security news, vulnerabilities, hacking, and research, including interviews with some of the top security professionals. Paul graduated from Bryant College with a degree in Computing and Information Systems, and is currently on the SANS GIAC advisory board. When not trying to hack something Paul can be found spending time with his wife and pug, Rocco.

Larry Pesce (CCNA, GCFA Silver, GAWN Gold) is the Manager for Information Services Security at a mid-sized healthcare organization in New England. In the last 13 years in the computer industry, Larry has become a jack of all trades; PC repair, network engineering, Web design, non-linear audio and video production and computer security. Larry is also gainfully employed as a Penetration Tester/Ethical Hacker with Defensive Intuition, a Rhode Island-based security consulting company. A graduate of Roger Williams University in Computer Information Systems, Larry is currently exploring his options for graduate education. In addition to his industry experience, Larry is also a Security Evangelist and co-host for the PaulDotCom Security Weekly podcast at www.pauldotcom.com. More of Larry's writing, guides and rants can be found on his blog at www.haxorthematrix.com and the SANS Reading Room.

Technical Editor

Raúl Siles is a senior Independent Security Consultant specializing in advanced security solutions and prevention, detection and response services in various industries including government, defense, telecom, manufacturing, and financial. Raul's expertise and service offerings include security architecture design and review, penetration testing, incident handling, forensic and malware analysis, network, system, database and application security assessments and hardening, code security reviews, wireless security, honeynets solutions, intrusion detection/prevention, expert witness, information security management and security awareness and training through The SANS Institute.

Contents

Chapter 1 WRT54G Fundamentals. 1

Introduction 2

Our Approach to This Book 2

History of the Linksys WRT54G 3

History of the WRT54G Open Source Firmware 4

Linksys WRT54G Series Hardware 4

WRT54G Series: Common Features 4

Power 5

The Reset Button 5

LED 5

Secure Easy Setup Button 6

Processor Architecture 7

Storage 9

Memory 10

Wireless and Ethernet Networking 11

Antenna Connectors 13

Determining Your Hardware Version 13

WRT54G Models 15

WRT54G, Version 1.0 16

WRT54G, Version 1.1 17

WRT54G, Version 2.0 19

WRT54G, Version 2.2 20

WRT54G, Versions 3.0 and 3.1 21

WRT54G, Version 4 22

WRT54G, Versions 5.0 and 6.0 24

WRT54G, Version 7.0 27

WRT54GL Models 27

WRT54GL, Version 1.0 28

WRT54GL, Version 1.1 28

Linksys WRT54GS Hardware 28

WRT54GS Models 28

WRT54GS, Version 1 30

WRT54GS, Version 1.1 30

WRT54GS, Version 2.0 31

WRT54GS, Version 2.1 31
WRT54GS, Version 3.0 32
WRT54GS, Version 4.0 32
WRT54GS, Versions 5.0, 5.1, and 6.0 33
Other Linksys WRT54G Hardware to Hack 34
WRT54GC Models 34
WRTSL54GS Models 34
WRT54G Buyer's Guide 38
Average User 40
Recommended Models 40
Recommended Firmware 42
Power User 43
Recommended Models 43
Recommended Firmware 44
Typical Geek 44
Recommended Models and Firmware 44
Speed Freak 45
Recommended Models and Firmware 45
Hardware Hacker 45
Recommended Models and Firmware 45
Penetration Tester 46
Recommended Models and Firmware 46
Bargain Shopper 46
Recommended Models and Firmware 46
Resources 48
Solutions Fast Track 49
Frequently Asked Questions 50

Chapter 2 Working with WRT54G Firmware 53

Introduction 54
Installing Third-Party Firmware 54
Installing Firmware via the Web Interface 55
Installing Firmware via TFTP 59
The Ping Hack 62
Using the Operating System nvram Command 63
Directly in the PMON/CFE 63
Linux TFTP Instructions 64
Windows TFTP Instructions 65

OS X TFTP Instructions .66

Completing the TFTP Installation .66

TFTP Firmware Installation Step by Step .67

Installing Firmware via JTAG .67

Introduction to Firmware Used in This Book .68

Linksys Original Firmware .68

Background .68

Features .68

Who Should Use This Firmware .68

Latest Linksys Firmware (VxWorks) .69

Background .69

Features .69

Who Should Use This Firmware .69

OpenWrt .69

Background .69

Features .70

Installation .70

Who Should Use This Firmware .76

DD-WRT .76

Background .76

Features .76

Installation .77

Who Should Use This Firmware .83

Ewrt .84

Background .84

Features .84

Who Should Use This Firmware .86

Other Firmware Worth Mentioning .86

FairuzaWRT .86

Background .86

Features .87

Installation .88

Using FairuzaWRT .89

Who Should Use This Firmware .96

Sveasoft .97

Background .97

Features .98

Who Should Use This Firmware 100
HyperWRT 100
Background 100
Features 101
Who Should Use This Firmware 104
Summary 105
Solutions Fast Track 105
Links to Sites 106
Frequently Asked Questions .107

Chapter 3 Using Third-Party Firmware 109

Introduction 110
Configuring and Using OpenWrt 110
The OpenWrt Command Line 110
Configuring OpenWrt Using nvram 111
Changing the IP Address .112
Installing Software with Ipkg 114
Installing Packages 116
Working with VLANs 117
Setting the Wireless Radio Transmit Power 119
Configuring the DNS and DHCP Server Using dnsmasq121
Configuring a Caching-Only DNS Server 122
Configuring a Custom DHCP Server 125
SSH Server Security 127
Reprogramming the SES Button As a WiFi Toggle 128
Configuring NTP Time Synchronization 129
Storage Using USB 131
Storage with Samba 132
Configuring a Samba Server 133
Configuring a Samba Client 135
Backing Up and Restoring .135
Installing and Using X-Wrt: A Web GUI for OpenWrt 137
Configuring and Using DD-WRT 141
Setting the Wireless Radio Transmit Power 141
Making the File System Writable 142
Working with VLANs 142
Securing Your Firmware 143
Securing OpenWrt 143

Disabling Telnet .145
Disabling HTTP and Enabling HTTPS .146
Disabling DNS and DHCP Servers .148
Verifying the Results .148
Securing DD-WRT .149
Disabling HTTP and Enabling HTTPS .149
Disabling Telnet and Enabling SSH .150
Disabling DHCP and DNS Servers .151
Keeping Up-to-Date .151
Summary .153
Resources .153
Solutions Fast Track .154
Frequently Asked Questions .155
Chapter 4 WRT54G Fun Projects 157
Introduction .158
Wardriving-in-a-Box .158
Prerequisites for This Hack .158
Kismet .158
The Finishing Touches .167
Setting Up a Wireless Media Adapter .171
Creating a Wireless Ethernet Bridge (WET) .171
Configuring the Bridge .172
Setting Up a Routed Bridge .175
Configuring the Firewall .177
Captive Portal-in-a-Box .178
Asterisk for VoIP .184
Installing Asterisk .184
Configuring Asterisk .185
Configuring modules.conf .185
Configuring VoIP Provider Connectivity .186
Configuring extensions.conf .190
Configuring the X-Lite Soft Phone .191
Troubleshooting Asterisk .193
Auto-Starting Asterisk on Boot .195
Summary .196
Solutions Fast Track .196
Frequently Asked Questions .197

Chapter 5 Securing Wireless Using a WRT54G. 199
Introduction 200
Basic Wireless Security 200
Select a Secure Network Name (SSID) 200
Hiding Your SSID 200
MAC Address Filtering 201
Configuring WEP 201
Configuring WPA-Personal (PSK) 202
Introduction to WPA/WPA2 (802.11i) 202
Configuring WPA-PSK (and WPA2-PSK) 204
Configuring WPA-Enterprise (and WPA2-Enterprise) 207
Access Point Configuration 209
Client Configuration 215
OS X Configuration 216
Windows Client Configuration 216
Finishing Up 218
Summary 219
Solutions Fast Track 219
Frequently Asked Questions 220

Chapter 6 WRT54G for Penetration Testers 223
Introduction 224
Tunneling and VPN 224
Using the WRT54G As an OpenVPN Bridged Client 225
Remote Office Connectivity with vpnc 229
Wireless Security Tools Using OpenWrt 233
WRT54G Kismet Drone 233
Installing and Configuring a Kismet Drone 234
WRT54G Remote Bluetooth Scanner 240
About the Bluetooth Adapter 240
Preparing the WRTSL54GS USB Capabilities 241
Configuring the USB Bluetooth Adapter 242
Using the USB Bluetooth Adapter to Discover Devices 243
WRT54G Remote 2.4GHz Spectrum Analyzer 249
WRTSL54GS CDMA Internet Connection 252
WRT54G Wireless Captive Portal Password Sniffer 257
Summary 264

Solutions Fast Track 264
Frequently Asked Questions 265

Chapter 7 WRT54G Hardware Hacking 267
Introduction 268
Fun with Wireless Antennas 268
Components Needed for This Hack 268
Understanding RF 268
Omnidirectional Antennas 269
Directional Antennas 270
Attaching Antennas to the WRT54G 271
Adding Ports: SD Card, Serial, and JTAG 273
Opening the Router 273
WRT54G and GL Series .273
WRTSL54GS Series 276
SD Card 276
Components Needed for This Hack 277
The Hack 277
Serial 291
Components Needed for This Hack 291
The Hack 292
JTAG 299
Components Needed for This Hack 300
The Hack 300
Constructing a JTAG Cable 301
Powering Your WRT54G with Alternative Sources 305
Components Needed for This Hack 305
The Hack 306
Alkaline Batteries 307
Rechargeable Lithium-ion Battery Pack 308
12 Volt Lead Acid Battery .309
Battery Comparison 310
USB 310
FireWire 400 311
Automotive Power 313
Homebrew Power over Ethernet (PoE) 314
Alternative Power Summary 316

Attaching Your WRT54G to Your Laptop 318
Component Needed for This Hack 318
The Hack 318
Summary 320
Solutions Fast Track 320
Frequently Asked Questions 322

Chapter 8 Troubleshooting WRT54G. 323
Introduction 324
Using OpenWrt Failsafe Mode to Unbrick Your Router . .324
Using JTAG to Unbrick Your Router 327
Getting Further Help 334
Resources for This Book 334
OpenWrt 334
DD-WRT 334
Ewrt 335
WRT54G Hacking Help 335
Summary 336
Solutions Fast Track 336
Frequently Asked Questions 337

Appendix A NVRAM Command Reference 339
Introduction 340
nvram Command Usage 340
IP and Networking 341
VLANs 342
Wireless 343
File System 347
Miscellaneous Hardware and Custom Software Options . . .347

Appendix B Hardware Hacking Parts 349
Introduction 350
Antennas 350
SD Card 350
Serial Port 351
JTAG 351
Alternative Power 352

Index 353

Chapter 1

WRT54G Fundamentals

Solutions in this chapter:

- Our Approach to This Book
- History of the Linksys WRT54G
- Linksys WRT54G Series Hardware
- WRT54G Buyer's Guide

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

The road to third-party firmware has been a long one, at least where the computer industry is concerned, and the changes to the WRT54G series of hardware have been many. In this chapter, we will discuss our approach to this book, the history of the WRT54G product line and its variations, and the history behind the development of third-party firmware.

Our Approach to This Book

This book is meant to document many of the features, projects, and interesting and fun things in general that you can do with the WRT54G series of routers from Linksys. Everyone should read this chapter in its entirety before moving on to other chapters in the book. Whether you own one WRT54G router or one of each model number in the series—or even if you have yet to purchase a WRT54G—you should read this chapter before reading any further. It will give you a map and a history of this hardware platform and it will help you to decide which model to purchase and/or whether your current hardware will do what you want it to do. If you do not yet own a WRT54G, or you just have an old dusty one in the corner, please note that we believe everyone should have at least two WRT54Gs at their disposal. Many of the projects we cover in this book either will require two routers, or will benefit performance-wise with at least two routers because you'll be able to split the processing load among them. And don't worry; the prices of these devices have come down over the years, making them affordable for even penny-pinching college students.

In this book, we have taken a "top-down" approach to teaching you how to make the most of the WRT54G platform. For instance, we show you by example how to configure and use these devices in various ways. In addition, we selected and documented each project and example carefully to ensure practical usage. Yes, we could show you how to use your WRT54G series router to run your entire Web site, database and all, but this is certainly not advisable. There are proper uses for your WRT54G, and there are some which stretch the limits so far that they are not practical. On the flip side of practical is, well, just plain fun, and we've made certain to include fun projects in this book as well. In each instance, we attempt to fully document the use case, based on extensive testing we've conducted in our own home and work environments. We included enough details about embedded devices, operating systems, and software engineering as we thought you would need, and we provide resources for those of you who want more details in these areas. We want this book to expand the audience of the WRT54G platform, and embedded device usage as a whole, unlocking the potential that this platform has to offer.

We want this book to be your road map to using WRT54G devices to your advantage in many different environments, including work and home. We've found so many uses for them that we know others can benefit as well. Hence, this book will guide you on your journey to unlocking all of the potential of the WRT54G hardware and software platforms.

NOTE

There are a few different perceived meanings of the word *hacking*. In this book, hacking means to use things for a purpose for which they were not originally intended. For example, Linksys did not intend to allow users to add a Secure Digital (SD) card reader to a WRT54G. However, we will show you how to "hack" the WRT54G and add an SD card reader to expand the WRT54G's storage capabilities. Hacking also refers to the act of gaining access to computer systems and/or networks (i.e., using the systems or software in a way that the creators did not originally intend), which should always be done with written permission. Along those lines, we will show you how to use WRT54G routers to aid in your legitimate hacking and security practices, such as penetration testing and performing network/system audits. You must always perform this testing with permission, preferably written, from appropriate parties.

History of the Linksys WRT54G

Linksys began selling version 1.0 of the WRT54G in late 2002 as a home router, firewall, and wireless networking product. In the beginning, it was primarily intended to support wireless networks, and inclusion of additional features merely complemented the wireless capabilities. At that time, the device was relatively commonplace; it featured a wide area network (WAN) port, a four-port 10/100 switch, and 802.11b support. The device also shipped with a Web interface for configuration—a practice that had become popular with consumer devices in earlier years. Since the initial launch in 2002, Linksys has revised the hardware of the WRT54G several times to provide upgrades to the base unit. The device has proven popular enough that Linksys has spawned several similar models in the WRT54G series to deliver various features, speed enhancements, and form factors. We will discuss a number of the models later in this chapter, and we will begin to see the natural progression that developments in technology have afforded the product line.

This particular product line has been a very good seller for Linksys. Although sales figures for the device are typically not broken out from sales figures for Linksys as a whole, company executives have been quoted as saying, "We sell literally hundreds of thousands per month." This popularity may be due, in part, to the ease with which you can modify the device, and as such a community of open source advocates and hardware hackers alike has embraced it readily.

With the recent official support from Linksys of third-party firmware through the release of the WRT54GL, Linksys is poised to sell even more units. We are currently seeing additional hardware revisions of the WRT54GL which, from an initial observation, seems to be following the trend of the original WRT54G series of hardware. With this continued development of the WRT54GL, and