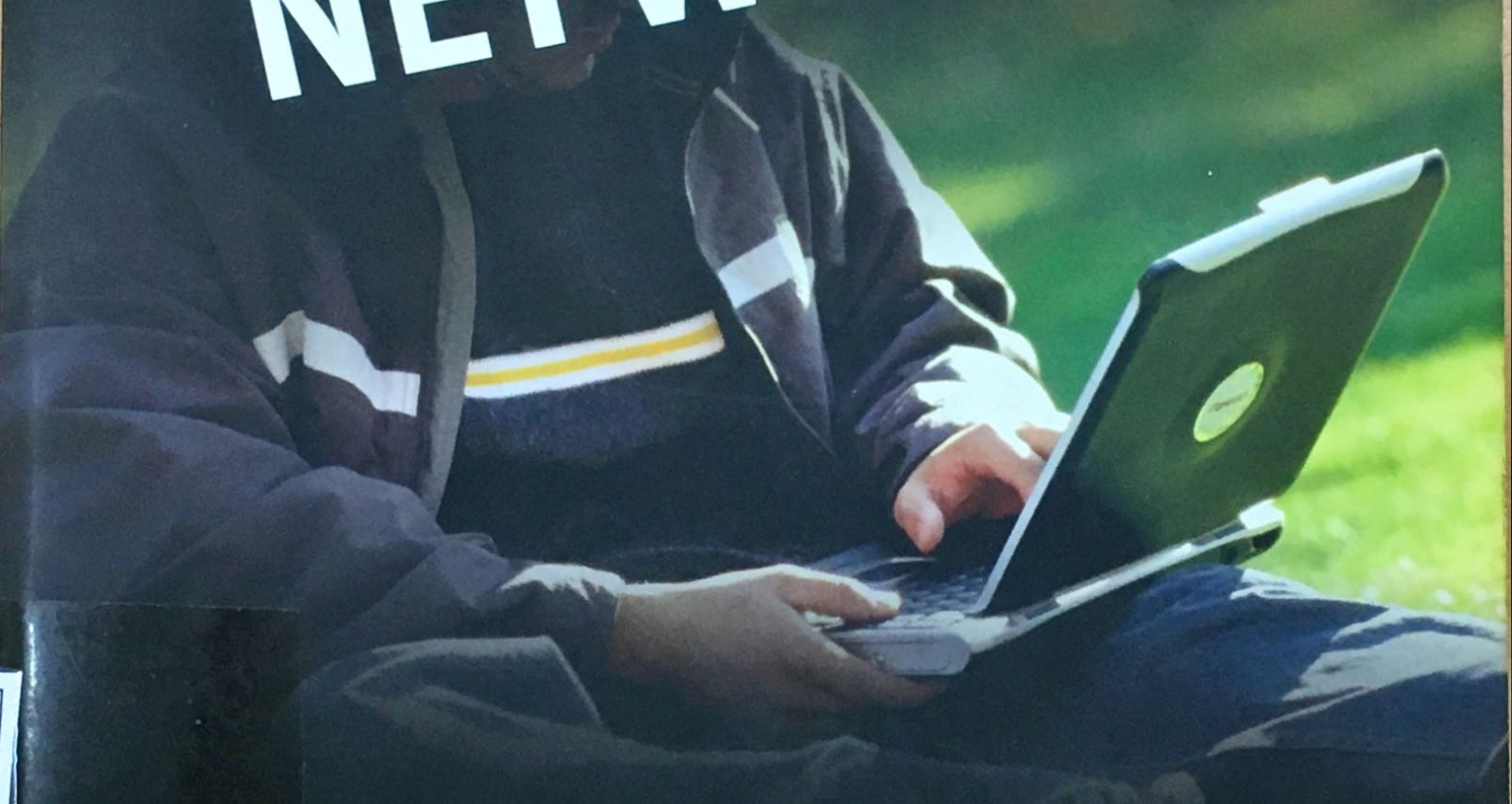


What you need to know to keep  
your information safe and secure

# CAUTION!

Jack McCullough

# WIRELESS NETWORKING



Preventing a Data Disaster

# CAUTION!



# **Caution! Wireless Networking: Preventing a Data Disaster**

# Caution! Wireless Networking: Preventing a Data Disaster



GIFT OF THE ASIA FOUNDATION  
NOT FOR RE-SALE

QUÀ TẶNG CỦA QUỸ CHÂU Á  
KHÔNG ĐƯỢC BÁN LẠI

Jack McCullough



WILEY

Wiley Publishing, Inc.



## Caution! Wireless Networking: Preventing a Data Disaster

Published by  
**Wiley Publishing, Inc.**  
111 River Street  
Hoboken, N.J. 07030  
www.wiley.com

Copyright © 2004 by Wiley Publishing, Inc., Indianapolis, Indiana

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data

ISBN: 0-7645-7213-X

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1MA/SS/QZ/QU/IN

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, E-Mail: brandreview@wiley.com.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEB SITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OF WEB SITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEB SITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.**

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

**Trademarks:** Wiley and the Wiley Publishing logo are trademarks or registered trademarks of John Wiley and Sons, Inc. and/or its affiliates. All other trademarks are the property of their respective owners. Wiley Publishing, Inc. is not associated with any product or vendor mentioned in this book.



WILEY is a trademark of Wiley Publishing, Inc.



## About the Author

Jack McCullough is the managing director of Razorwire Information Security Consulting. His technical expertise includes wireless and wired networks, computer security, physical security, programming, cryptography, and technical curriculum development. Jack's background includes ten years of experience in the IT field. He has held positions as IT director, operations manager, network administrator, programmer, and software trainer. A respected IT and security authority, he is frequently sought out for informational interviews by both broadcast and print media services.

Jack has authored books, magazine articles, and white papers on computer security; his written works have been translated into several languages. Many universities have used his books and white papers in information security courses, as have the governments of Australia, the Peoples Republic of China, Japan, Brazil, and Taiwan. Jack continues to actively research information security, discover new ways to exploit the weaknesses in networked systems, and determine best practices that enable the average computer user to address these threats in an efficient manner.

When he isn't writing about or researching technology, Jack teaches karate and self-defense under the watchful eyes of Sensei Floyd Burk, and Sensei Martha Burk at the Alpine Karate Academy in Alpine, California, and practices writing about himself in third-person.

# Credits

**Acquisitions Editor**  
Mike Roney

**Project Editor**  
Cricket Krengel

**Technical Editor**  
Greg Guntle

**Copy Editor**  
Kim Heusel

**Editorial Manager**  
Robyn Siesky

**VP & Publisher**  
Barry Pruett

**Vice President & Group  
Executive Publisher**  
Richard Swadley

**Project Coordinator**  
Maridee Ennis

## **Graphics and Production Specialists**

Karl Brandt  
Jonelle Burns  
Amanda Carter  
Carrie A. Foster  
Lauren Goddard  
Jennifer Heleine

## **Quality Control Technicians**

Susan Moritz  
Carl William Pierce  
Brian H. Walls

**Proofreading**  
Christine Sabooni

**Indexing**  
Johnna VanHoose



# Acknowledgments

*To Cathy, for her support during this  
and all of my other projects.*

# Acknowledgments

---

It takes a lot of exceptional people to complete a project like this. First and foremost, a big thank you goes to my literary agent, David Fugate of Waterside productions, arguably the best agent working for technical authors today. I want to thank Mike Roney for sharing his vision for the book and hiring me to write it, and my development editor, Cricket Krengel, who expertly guided me through preparing this manuscript and put so much work into editing it — especially after the vision of the title changed and we had to rethink several chapters. Finally, thanks to the layout and production team at Wiley for putting this book together and for interpreting my scribbles into actual art that the reader can understand.



# Contents at a Glance

Acknowledgments . . . . .	ix
<b>Part I: Understanding the Threat . . . . .</b>	<b>1</b>
Chapter 1: A Brief Overview of Wi-Fi . . . . .	3
Chapter 2: Network Fundamentals and Security Concerns . . . . .	23
Chapter 3: The People behind the Problem . . . . .	45
Chapter 4: Hijacking Wi-Fi . . . . .	59
Chapter 5: More Wireless Attacks . . . . .	77
Chapter 6: Wardriving . . . . .	89
Chapter 7: Viruses and Wi-Fi . . . . .	101
<b>Part II: Protecting Yourself . . . . .</b>	<b>123</b>
Chapter 8: Technical Pitfalls and Solutions . . . . .	125
Chapter 9: Wireless Privacy Concerns . . . . .	147
Chapter 10: Encryption and Wi-Fi . . . . .	167
Chapter 11: Securing Your WLAN . . . . .	187
Chapter 12: Protecting Your Wi-Fi Data . . . . .	217
Appendix A: Suppliers, Manufacturers, and Resources . . . . .	233
Appendix B: Wireless Standards . . . . .	243
Glossary . . . . .	249
Index . . . . .	257



# Contents

Acknowledgments . . . . .	ix
---------------------------	----

## Part I: Understanding the Threat 1

### Chapter 1: A Brief Overview of Wi-Fi . . . . . 3

Introducing Wi-Fi . . . . .	3
What is wireless networking? . . . . .	4
Comparing wireless and Ethernet . . . . .	5
How Wi-Fi works . . . . .	9
Examining Wi-Fi Equipment . . . . .	11
Looking at access points . . . . .	11
Checking out adapters . . . . .	13
Equipment Worth Avoiding . . . . .	14
Skipping defunct standards . . . . .	14
Passing on nonupgradeable gear . . . . .	15
Demystifying Wireless Standards . . . . .	15
Introducing 802.11: At the base of it all . . . . .	16
Explaining 802.11b . . . . .	16
Comparing 802.11a . . . . .	17
Speeding up with 802.11g . . . . .	17
Better security with 802.11i . . . . .	17
Speeding toward the future with 802.11n . . . . .	18
Expanding with Bluetooth and 802.15.1 . . . . .	18
Introducing Organizations and Certification . . . . .	20
Meeting the Wi-Fi Alliance . . . . .	20
Introducing the IEEE . . . . .	21
Summary . . . . .	21

### Chapter 2: Network Fundamentals and Security Concerns. . . . . 23

Explaining networking terms . . . . .	23
Node . . . . .	24
Protocol . . . . .	24
Network . . . . .	24
Internetwork, Internet, intranet . . . . .	25
Host . . . . .	26
Server . . . . .	26
Client . . . . .	26



Service . . . . .	26
Workstation . . . . .	27
Peer . . . . .	27
Examining Network Models . . . . .	27
Deconstructing the OSI reference model . . . . .	27
Comparing the TCP/IP model . . . . .	29
Examining Wi-Fi layers . . . . .	31
Demystifying the TCP/IP protocols . . . . .	32
Defining important protocols . . . . .	32
Understanding packet switching and encapsulation . . . . .	33
Understanding Network Addresses and Names . . . . .	35
Explaining IP addresses . . . . .	35
Demystifying address classes . . . . .	35
Exposing restricted addresses . . . . .	36
Explaining subnets . . . . .	36
Masking subnets . . . . .	38
Dynamic host configuration protocol . . . . .	38
Domain names . . . . .	39
Root domains . . . . .	40
Subdomains and host names . . . . .	40
Connecting Networks . . . . .	40
Network bridges . . . . .	41
Routers and gateways . . . . .	41
Summary . . . . .	43

## Chapter 3: The People Behind the Problem . . . . . 45

Separating Hackers from Crackers . . . . .	45
Meeting the white hats . . . . .	46
Avoiding the black hats . . . . .	47
Understanding the gray hats . . . . .	47
Identifying script kiddies . . . . .	47
Hacktivists . . . . .	49
Visiting the Underground Cracker Culture . . . . .	50
What Makes Hackers and Crackers Tick . . . . .	51
Looking for knowledge . . . . .	51
Fulfilling greed . . . . .	52
Inflating their egos . . . . .	52
Pursuing revenge . . . . .	52
Hacker Conventions and Gatherings . . . . .	53
DEFCON . . . . .	53
HOPE . . . . .	53
ToorCon . . . . .	54
2600 meetings . . . . .	54
Worldwide Wardrive . . . . .	54