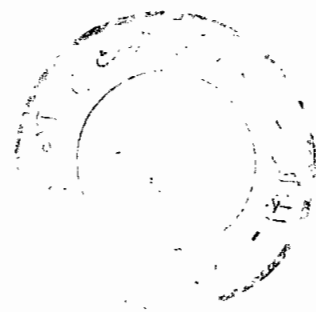


Caution! Wireless Networking: Preventing a Data Disaster

BIBLIOTHEQUE DU CERIST





Caution! Wireless Networking: Preventing a Data Disaster

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.

7758

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

BIBLIOTHEQUE DU CERIST

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

BIBLIOTHEQUE DU CERIST

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

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

Part I: Understanding the Threat 1

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

Part II: Protecting Yourself 123

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

Examining Crackers' Tricks	54
Social engineering	55
Trashing	56
Entertaining Hacking/Cracking Resources	57
Summary	58
Chapter 4: Hijacking Wi-Fi	59
Hijacking Sessions	59
Spoofing	60
Explaining race conditions	64
Public hotspots	64
Protecting yourself at hotspots	65
Exposing the man in the middle	68
Understanding Rogue Access Points	68
Uncovering Denial of Service Attacks	70
WPA denial of service	72
Disassociate frame attack	73
Strong signal jamming	73
FakeAP flood	74
Summary	75
Chapter 5: More Wireless Attacks	77
Attacking Hosts	77
Using OS weaknesses	79
Using known security issues	83
Sniffing the Network	85
How sniffing works	86
The promiscuous NIC	87
Summary	88
Chapter 6: Wardriving	89
Introducing Wardriving	89
How wardriving works	91
Hiding your network	91
Changing default settings	92
Avoiding DHCP	94
Filtering network traffic	95
Using encryption	95
Legality of wardriving	96
Warchalking	97
Warspying	98
Software for Defense	99
More About Wardriving	100
Summary	100

Chapter 7: Viruses and Wi-Fi 101

Understanding Malicious Software	101
Examining Computer Viruses	104
Dangerous and double extensions	106
The Microsoft fink-fund	109
Exposing Trojan Programs	110
Discovering Internet Worms	111
Discovering Blended Threats	114
Bot Software	116
Introducing Spyware	118
Investigating Viruses on Handhelds	120
Understanding the Hoax Problem	120
Summary	122

Part II: Protecting Yourself 123**Chapter 8: Technical Pitfalls and Solutions 125**

Discovering Common Wi-Fi Problems	125
Explaining multipath interference problems	125
Adjacent channels overlapping	130
Identifying theft of service	131
Uncovering configuration errors	132
Detecting and Dealing with Interference	134
Identifying interference in your home or office	135
Identifying interference outside your home or office	135
Avoiding physical barriers	136
Defining Interoperability Issues	138
Learning About Antennas	138
Improper mounting	140
Grounding antennas	142
Delineating the Fresnel zone	143
Interference from trees	144
Optimizing Equipment	145
Summary	146

Chapter 9: Wireless Privacy Concerns 147

Why Privacy Matters	147
Wi-Fi Privacy Threats	149
Understanding location-based services	149
Exposing spyware	151
Avoiding adware and drive-by downloads	152
Tossing your cookies for greater privacy	154

Demystifying Privacy Policies	156
Other Vulnerable Wireless Technology	158
Intercepting X10 device signals	158
Peeping in on Wi-Fi video cameras	161
Eavesdropping on cordless phones	163
Summary	165
Chapter 10: Encryption and Wi-Fi	167
Introducing Encryption	167
The crypts	168
Cipher	168
Plaintext	168
Ciphertext	170
Encryption key	170
A very brief history of encryption	171
Secret keys	172
Understanding Modern Encryption Techniques	173
Failings of secret key cryptography	173
Understanding public key cryptography	174
Examining hybrid systems	175
Digital signatures	176
Digital certificates	177
Entropy and key strength	178
Debunking Wired Equivalent Privacy (WEP)	179
Understanding why WEP fails	179
Why you should still use WEP	180
Investigating Wi-Fi Protected Access (WPA)	182
Introducing Pretty Good Privacy (PGP)	184
Summary	185
Chapter 11: Securing Your WLAN	187
Understanding WLAN Vulnerabilities	187
Changing Dangerous Default Settings	188
Rethinking the SSID	188
Changing passwords and usernames	190
Editing IP addresses	191
Understanding DHCP	193
Understanding why DHCP can be a problem	194
Assigning static IP addresses	195
Filtering Network Traffic	197
Activating MAC address filtering	199
Implementing IP address filtering	201

Modifying Broadcast Parameters	202
Adjusting the power	203
Turning off SSID broadcast	204
Setting a minimum connection speed	205
Using Encryption	205
Using WEP	205
Installing WPA firmware upgrades	206
Securing Clients and Hosts	207
Locking down Windows XP	208
More steps to secure your XP machine	213
Disabling unnecessary services	214
Summary	215
Chapter 12: Protecting Your Wi-Fi Data	217
Identifying Threats to Wireless Data	217
Examining hardware failure	218
Exposing outside threats to data	218
Choosing backup systems	219
Determining what you need to back up	219
Deciding how often you will back up	220
Choosing a type of storage	220
Selecting media for backups	223
Things you should consider	224
Backing up via the Internet	225
Backup software	226
Protecting Your Hardware	228
Surge and spike protection	228
Lightning arrestors and grounding antennas	229
Preventing problems through proper maintenance	230
Summary	232
Appendix A: Suppliers, Manufacturers, and Resources	233
Wi-Fi Networking Hardware	233
Wi-Fi Resources	236
Security, Privacy, and Antivirus Resources	238
PDA, PC, and Accessory Manufacturers	240
Software	241
Appendix B: Wireless Standards	243
Glossary	249
Index	257