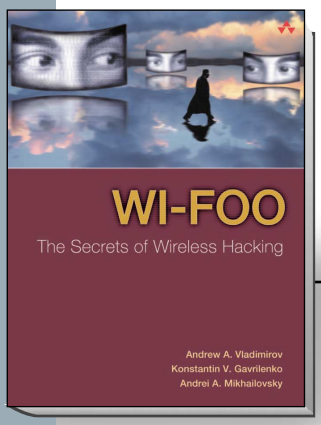
**The definitive guide to penetrating and defending wireless networks**




ANDREW A. VLADIMIROV
KONSTANTIN V. GAVRILENKO
ANDREI A. MIKHAILOVSKY

# WI-FOO

## The Secrets of Wireless Hacking

Straight from the field, this is the definitive guide to hacking wireless networks. Authored by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack — or protect — any wireless network.

The authors introduce the "battlefield," exposing today's "wide open" 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools; crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless "citadels" — including cryptography-based techniques, authentication, wireless VPNs, intrusion detection, and more.

©2004, Paper, 608 pages,
0-321-20217-1, $34.99

**If you're a hacker or security auditor, this book will get you *in*. If you're a netadmin, sysadmin, consultant, or home user, it'll keep everyone else *out*.**

### Coverage Includes

- Step-by-step walkthroughs and explanations of wireless-specific attacks
- Building wireless hacking/auditing toolkit: detailed recommendations, ranging from network discovery tools to client cards chipsets and antennas
- Wardriving: network mapping and site surveying
- Potential weaknesses in current and emerging security protocols, including 802.11i, PPTP,and IPSec
- Implementing strong, multilayered defenses
- Wireless IDS: why attackers aren't as untraceable as they think
- Wireless hacking and the law: what's legal, what isn't

### About the Authors

**ANDREW A.VLADIMIROV** leads the wireless consultancy division at Arhont Ltd, one of the UK's leading security consultants. He was one of the UK's first IT professionals to obtain the coveted CWNA wireless certification.

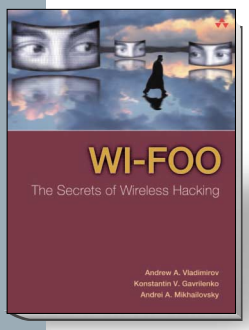
**KONSTANTIN V. GAVRILENKO** co-founded Arhont Ltd. His 12+ years' IT and security expertise includes wireless security, firewalls, cryptography, VPNs, and IDS.

**ANDREI A. MIKHAILOVSKY** has more than a decade of networking and security experience and has contributed extensively to Arhont's security research papers.

**THE AUTHORS** have been active participants in the IT security community for many years and are security testers for leading wireless equipment vendors.

Addison Wesley

## Table of Contents




Introduction

CHAPTER 1 Real World Wireless Security
CHAPTER 2 Under Siege
CHAPTER 3 Putting the Gear Together: 802.11 Hardware
CHAPTER 4 Making the Engine Run: 802.11 Drivers and Utilities
CHAPTER 5 Learning to War Drive: Network Mapping and Site Surveying
CHAPTER 6 Assembling the Arsenal: Tools of the Trade
CHAPTER 7 Planning the Attack
CHAPTER 8 Breaking Through
CHAPTER 9 Looting and Pillaging: The Enemy Inside
CHAPTER 10 Building the Citadel: An Introduction to Wireless LAN Defense
CHAPTER 11 Introduction to Applied Cryptography: Symmetric Ciphers
CHAPTER 12 Cryptographic Data Integrity Protection, Key Exchange, and User Authentication Mechanisms
CHAPTER 13 Fortress Gates: User Authentication in Wireless Security
CHAPTER 14 Guarding the Airwaves: Deploying Higher Layers Wireless VPNs
CHAPTER 15 Counterintelligence: Wireless IDS Systems

Appendix A Decibel – Watts Conversion Table
Appendix B 802.11 Wireless Equipment
Appendix C Antenna Types
Appendix D Wireless Utilities Manpages
Appendix E Signal Loss for Obstacle Types
Appendix F Warchalking Signs
Appendix G Penetration Testing Template
Appendix H Default SSIDs for Several Common 802.11 Access Point and PCMCIA Card Products

Glossary

Addison Wesley

**ORDERING INFORMATION:**

SINGLE COPY SALES:
Visa, Master Card, American Express, Checks, or Money Orders only —
Tel: 515-284-6761
Fax: 515-284-2607
Toll-Free: 800-811-0912

GOVERNMENT AGENCIES:
Kathryn Bass
GS-14F-8023A
703-404-9194
www.pearsongovernmentsales.com

COLLEGE PROFESSORS:
Desk or Review Copies —
exam@aw.com

CORPORATE ACCOUNTS:
Quantity, Bulk Orders totalling 10 or more books. Purchase orders only — No credit cards.
Fax: 317-428-3343
Toll-Free: 800-382-3419

**INTERNATIONAL ORDERING INFORMATION:**

CANADA:
cdn.ordr@pearsoned.com

UK/EMEA:
*Europe, Middle East, South Africa*
de-order@pearson.com

BENELUX:
amsterdam@pearsoned-ema.com

AUSTRALIA:
trade@pearsoned.com.au

SOUTH ASIA:
asia@pearsoned.com.sg

NORTH ASIA:
misip@pearsoned.com.hk

OTHER REGIONS:
tim.galligan@pearsoned.com