802.11安全手册(影印版)

802.11 Security

Bruce Potter & Bob Fleck 著

O'REILLY®

清华大学出版社

802.11 安全手册（影印版）

802.11 Security

Bruce Potter & Bob Fleck

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权清华大学出版社出版

清华大学出版社

图书在版编目（CIP）数据

802.11 安全手册: /（美）波特（Potter, B.）,（美）弗利克（Fleck, B.）著 — 影印版 . — 北京:
清华大学出版社，2003.6
书名原文：802.11 Security
ISBN 7-302-06534-9

Ⅰ.8... Ⅱ.①波... ②弗... Ⅲ.无线电通信 - 通信网 - 安全技术 - 技术手册 - 英文 Ⅳ.TN92-62

中国版本图书馆 CIP 数据核字（2003）第 025950 号

北京市版权局著作权合同登记
图字：01-2003-1926 号

书　　名/ 802.11 安全手册（影印版）
书　　号/ ISBN 7-302-06534-9/TP · 4901
责任编辑/ 常晓波
封面设计/ Emma Colby，张健
出版发行/ 清华大学出版社（www.tup.tsinghua.edu.cn）
地　　址/ 北京清华大学学研大厦（邮政编码 100084）
经　　销/ 各地新华书店
印　　刷/ 北京艺辉印刷有限公司
开　　本/ 787 毫米 × 980 毫米　16 开本　12.25 印张
版　　次/ 2003 年 6 月第一版　2003 年 6 月第一次印刷
印　　数/ 0001-3000 册
定　　价/ 21.00 元（册）

O'Reilly & Associates公司介绍

O'Reilly & Associates公司是世界上在UNIX、X、Internet和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的*The Whole Internet User's Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly & Associates一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates依靠他们及时地推出图书。因为O'Reilly & Associates紧密地与计算机业界联系着，所以O'Reilly & Associates知道市场上真正需要什么图书。

Preface

From the early days of wireless communication, the ability to transmit news, thoughts, and feelings without wires has revolutionized our daily lives. The radio broadcasts of the 1920s brought instant news and entertainment to households all over the world. The adoption of television in the 1950s added a visual aspect to the experience. CB radio made a big impact in the 1970s, allowing individuals within a limited distance to talk with each other while on the road. In the 1980s, cellular phones and pagers allowed people to be connected to their home or office no matter where they were. Now at the start of the 21st century, low-cost, high-speed wireless data networking has become a reality. Anyone can go to his or her local computer store and easily purchase wireless networking equipment that can transmit packet-based data at millions of bits per second.

Throughout the entire process, the integrity and confidentiality of the information traveling through the air has always been a concern. Who is *really* broadcasting the signal you are receiving? Is anyone eavesdropping on the signal? How can you make sure that an eavesdropper is unable to obtain useful information from the signal? These questions are not particularly important when you are watching television but become critical when you are transmitting data between military installations or making a stock transaction over the Internet using your 802.11b-capable PDA. Due to the ease with which an attacker can intercept or modify your 802.11b communications, it is imperative that you understand the risks in using a wireless network and how to protect yourself, your infrastructure, and your users.

Assumptions About the Reader

This book is aimed at network engineers, security engineers, systems administrators, or general hobbyists interested in deploying secure 802.11b-based systems. Primarily, the discussions in this book revolve around Linux and FreeBSD. However, there is a great deal of general-purpose information as well as tips and techniques for Windows users and users of firmware-based wireless access points.

The book assumes the reader is familiar with the installation and maintenance of Linux or FreeBSD systems. The techniques in the book rely heavily on custom kernel configuration, startup scripts, and general knowledge of how to configure the operating systems. We provide links and references to resources to help with these issues but do not address then directly. This book concentrates on the issues germane to wireless security and leaves the operating-system-specific installation procedures as an exercise to the user.

The reader is also assumed to be familiar with general networking concepts. The reader should understand, at least at a high level, concepts such as the OSI layers, IP addressing, route tables, ARP, and well-known ports. We feel this makes the book more readable and useful as a guide for *wireless* networks, not networks in general. Again, we attempt to provide references to other resources to assist readers who may be unfamiliar with these topics.

Scope of the Book

This book attempts to give you all the knowledge and tools required to build a secure wireless network using Linux and FreeBSD. You will be able to use this book as a roadmap to deploy a wireless network; from the client to the access point to the gateway, it is all documented in the book. This is accomplished by a two-step process. First, we talk about wireless and 802.11b in general. This book will give you a broad basis in theory and practice of wireless security. This provides you with the technical grounding required to think about how the rest of the book applies to your specific needs and situations.

The second part of this book details the technical setup instructions needed for both operations systems including kernel configurations and various startup files. We approach the specific technical setup using a "from the edge to the core" concept. We start by examining the security of a wireless client that is at the very edge of the network. Then, we move toward the core by providing a method of setting up a secure access point for client use. From there, we move even farther toward the core by examining secure configuration of the network's IP gateway. Finally, we zoom all the way out and discuss security solutions that involve many parts of the network, including end-to-end security.

Part I, *802.11 Security Basics*, provides an introduction to wireless networks and the sorts of attacks the system administrator can expect.

Chapter 1, *A Wireless World*, introduces wireless networking and some high-level security concerns. The chapter talks briefly about basic radio transmission issues such as signal strength and types of antennas. It also examines the differences and similarities between members of the 802.11 suite of protocols. Finally, we discuss the Wired Equivalency Protocol (WEP) and its weaknesses.

Chapter 2, *Attacks and Risks*, examines the types and consequences of attacks that can be launched against a wireless network. This chapter opens with a discussion of denial-of-service attacks, proceeds to man-in-the-middle attacks, and finishes with a section on illicit use of network resources.

Part II, *Station Security*, shows you how to lock down a wireless client machine such as a laptop. These chapters contain general security best practices for workstations (which are, unfortunately, rarely used). They also contain specific wireless kernel, startup, and card configuration. Finally, we provide tactics for stopping attackers on the same wireless network as well as how to audit the entire workstation.

Chapter 3, *Station Security*, discusses the general approach and concerns for securing a wireless client. This chapter provides a foundation for the five OS-specific chapters that follow it.

Chapter 4, *FreeBSD Station Security*, discusses specific concerns for securing a FreeBSD wireless client. This chapter discusses kernel, interface, and operating system configuration issues. It also presents techniques and tools for detecting various attacks and defending against them.

Chapter 5, *Linux Station Security*, discusses specific concerns for securing a Linux wireless client. Kernel, interface, and operating system configuration issues are presented. This chapter also presents techniques and tools for detecting various attacks and defending against them including a basic firewall configuration.

Chapter 6, *OpenBSD Station Security*, discusses specific concerns for securing an OpenBSD wireless client. This chapter discusses kernel, interface, and operating system configuration issues that are unique to OpenBSD. It also presents techniques and tools for detecting various attacks and defending against them.

Chapter 7, *Mac OS X Station Security*, shows how to securely configure a Mac OS X wireless client. Techniques for hardening the operating system as well as firewall configurations are presented in this chapter.

Chapter 8, *Windows Station Security*, provides a brief discussion of securing a Microsoft Windows wireless client. Basic ideas such as anti-virus software and firewall options are covered in this chapter.

Part III, *Access Point Security*, covers the configuration and security of access points.

Chapter 9, *Setting Up an Access Point*, shows how to install and securely configure a wireless access point. This chapter starts with a discussion of generic security problems occurring on most access points, especially firmware access points commonly available at computer stores. We also describe the installation and secure configuration of the HostAP drivers for Linux, FreeBSD, and OpenBSD.

Part IV, *Gateway Security*, covers the more complex issue of gateway configuration on several platforms.

Chapter 10, *Gateway Security*, discusses the general issues related to the configuration and deployment of the network gateway. The discussion in this chapter frames the concerns that will be addressed using the configuration guides of the three chapters that follow it.

Chapter 11, *Building a Linux Gateway*, provides the steps necessary to install and configure a properly secured IP gateway for a wireless network. The chapter discusses how to install the operating system and bring up all of the network interfaces. From there, firewall rules are presented with an explanation of why each rule is necessary. Finally, installation and configuration of supporting services such as DHCP and DNS are provided.

Chapter 12, *Building a FreeBSD Gateway*, is similar to Chapter 11 except the configurations and suggestions are for FreeBSD.

Chapter 13, *Building an OpenBSD Gateway*, is similar to Chapter 11 except the configurations and suggestions are for OpenBSD.

The remainder of the book covers technologies and techniques that can be used across the entire network.

Chapter 14, *Authentication and Encryption*, covers supplementary tools that can help secure wireless network traffic. This chapter examines the use of portals to control network access. Next, we examine the use of 802.1x and VPNs to secure the network.

Chapter 15, *Putting It All Together*, examines the interplay between the clients, access points, and gateways. This chapter opens with a discussion of how the users affect the architecture of the network. Finally, we attempt to look into the crystal ball and determine what the future holds for wireless security.

Conventions Used in This Book

- *Italic* is used for commands, directory names, filenames, scripts, emphasis, and the first use of technical terms.
- `Constant width` is used for IP addresses, network interfaces, partitions, and references to code in regular text.
- *`Constant width italic`* is used for replaceable text.
- ***`Constant width bold italic`*** is used for user input.

Pay special attention to notes set apart from the text with the following icons:

This is a tip. It contains useful supplementary information about the topic at hand.

This is a warning. It helps you solve and avoid annoying problems.

Other Sources of Information

Wireless security is a dynamic field of study. It is important to know where to obtain the latest information on wireless technologies as well as information on the latest attacks. At the time of this writing, there are many standards under development that may drastically change the wireless landscape within the next few years. In addition, the features provided in each operating system are being enhanced and expanded constantly, so it is important to know how those changes impact your deployment.

More links can be found at: *http://www.dailywireless.org*.

Standards and References

IEEE 802 Standards Online is at *http://standards.ieee.org/getieee802/*.

The Wireless Ethernet Compatibility Alliance is at *http://www.wirelessethernet.org/*.

Operating-System-Specific Documentation

Linux Netfilter documentation is at *http://www.netfilter.org*.

The HostAP driver for Linux is at *http://hostap.epitest.fi*.

The FreeBSD Handbook is at *http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html*.

Mailing Lists

The bugtraq mailing list is a primary source for breaking news on software vulnerabilities. The vuln-dev mailing list occasionally has in-depth discussions on security problems with wireless networks. Both can be subscribed to at *http://www.securityfocus.com*.

We'd Like to Hear from You

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!). Please let us know about any errors you find, as well as your suggestions for future editions, by writing to:

O'Reilly & Associates, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

(800) 998-9938 (in the United States or Canada)
(707) 829-0515 (international/local)
(707) 829-0104 (fax)

We have a web page for this book where we list examples and any plans for future editions. You can access this information at:

http://www.oreilly.com/catalog/80211security

You can also send messages electronically. To be put on the mailing list or request a catalog, send email to:

info@oreilly.com

To comment on the book, send email to:

bookquestions@oreilly.com

Acknowledgments

The authors would like to thank their editor, Jim Sumser, for his effort in making this book as clear and useful as possible. We would also like to thank him for his assistance throughout the process of writing this, including giving us the freedom to tackle the book in our own unique way.

Many insightful suggestions were provided during the review process, and we want to extend our deepest thanks to the reviewers: Bob Abuhoff, Agoussi Amon, Dave Markowitz, and John Viega.

Special thanks to Matt Messier for providing information and the firewall scripts for Mac OS X.

We would also like to thank O'Reilly & Associates for giving us the opportunity to write this book.

From Bruce Potter

I would first like to thank my wife, Heidi, and two children, Terran and Robert (who was born halfway through the writing process). They gave me the time and support needed to research and write this book. Without them, I never would have made it.

I would also like to thank the members of NoVAWireless for their expertise and never-ending pursuit of knowledge. Through technical and non-technical discussions on the mailing list, I have learned a great deal of information that helped me with this book.

Finally, I would like to thank The Shmoo Group and in particular, Adam Shand of PersonalTelco. You guys and gals have been the foundation for much of my technical work for the last few years.

From Bob Fleck

I would like to thank my parents for their encouragement and support of both my education and my exploration of computers as I grew up. Many thanks also to my uncle, Chris Fleck, who has fostered my interest in computer science since shortly after I learned to read.

The advice and knowledge of my coworkers and colleagues has been priceless. John Viega helped by guiding me through the trials of writing a book. Will Radosevich, Jordan Dimov, and Jose Nazario have all been a great help over the last few years as a source of discussions on wireless networking and security.

The community wireless networking groups around the world have made great contributions to understanding the uses of these technologies and developing interesting ways of deploying and securing 802.11 networks. I can't thank them enough for the knowledge they have collected on their websites and mailing lists. Just as important, I thank the ISPs that actively support wireless networking and cooperate with their customers to explore the new possibilities it provides.

Table of Contents

Part I. 802.11 Security Basics

Part II. Station Security

Part III. Access Point Security

Part IV. Gateway Security

PART I

802.11 Security Basics

The phrase "wireless security" is considered by some to be an oxymoron. How can a system with no physical security hope to facilitate secure data transport? Well, with careful planning and configuration, a wireless network can protect itself from many types of attacks and become almost as secure as its wired counterpart. 802.11 can be deployed with various security mechanisms to provide robust, mobile, and hardened network infrastructure. In order to understand how and when to use the security tools at hand, you must first understand the underlying structure of the 802.11 protocol as well as the risks associated with deploying and using a wireless network. The following chapters will provide the basic grounding in how the 802.11 protocols work, the inherent security mechanisms it has, and how an attacker will attempt to exploit weak spots within a wireless network.