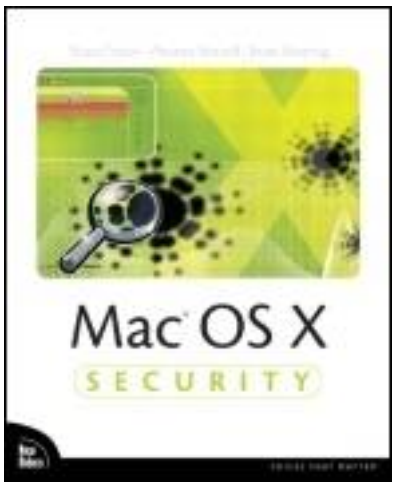


- Table of Contents
- Index

Mac® OS X Security

By Bruce Potter, Preston Norvell, Brian Wotring

START READING

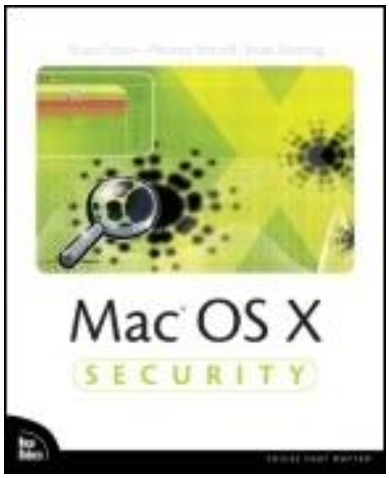
Publisher: New Riders Publishing

Pub Date: May 23, 2003

ISBN: 0-7357-1348-0

Pages: 0

Mac OS X now operates on a UNIX engine. As such it is much more powerful than previous operating systems. It is now a multitasking, multithreaded, multi-user, and multiprocessor system with enhanced interoperability with other systems. Along with that increased power comes increased security vulnerability. Part I introduces readers to the basics of OS X security. Part II addresses system security beginning at the client workstation level. This section addresses UNIX-specific information such as permissions, executables, and network protocols and the related security concerns. Part III covers network security. The chapters in this section will cover security for internet services, file sharing, and network protection systems. Part IV addresses enterprise security using a variety of tools (Kerberos, NetInfo, and Rendezvous) as well as workstation configurations to illustrate how OS X Server and OS X inter-operate. The final section addresses auditing and forensics and what to do when an OS X network is compromised. This section teaches readers to audit systems painlessly and effectively and how to investigate and handle incidents.



Mac® OS X Security

By Bruce Potter, Preston Norvell, Brian Wotring

START READING

Publisher: New Riders Publishing

Pub Date: May 23, 2003

ISBN: 0-7357-1348-0

Pages: 0

Copyright

Library of Congress Catalog Card Number: 2002115258

Printed in the United States of America

First edition: June 2003

06 05 04 03 7 6 5 4 3 2 1

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit number is the number of the book's printing. For example, the printing code 03-1 shows that the first printing of the book occurred in 2003.

Trademarks

Warning and Disclaimer

ASSOCIATE PUBLISHER: Stephanie Wall

MANAGING EDITOR: Gina Kanouse

SENIOR PRODUCT MARKETING MANAGER: Tammy Detrich

PUBLICITY MANAGER: Susan Nixon

SENIOR ACQUISITIONS EDITOR: Linda Anne Bump

Development Editor: Chris Zahn

Senior Project Editor: Lori Lyons

Copy Editor: Linda Seifert

Senior Indexer: Cheryl Lenser

Proofreader: Teresa Stephens

Interior Design: Wil Cruz

Composition: Wil Cruz Jake McFarland

Manufacturing Coordinator: Dan Uhrig

Cover Designer: Aren Howell

Dedication

Bruce Potter

To my family.

Preston Norvell

To my Grandfathers all.

Brian Wotring

To my grandparents, Lyle and Mary Goodspeed.

PREVIOUS NEXT

About the Authors

Bruce Potter has a broad information security background. From application security assessments to low-level smartcard analysis to wireless network deployments, Bruce has worked in both the open- and closed-source communities. Trained in computer science at the University of Alaska Fairbanks, Bruce served as a senior technologist at several high-tech companies in Alaska and Virginia. He currently is employed as a Senior Software Security consultant with Cigital Inc. in Dulles, Virginia. Bruce is founder and President of Capital Area Wireless Network, a non-profit based in Washington, DC. CAWNet, an organization of community members and commercial wireless Internet Service Providers (WISPs), is attempting to create a large-scale public wireless network throughout the metro-DC area. In 1999 Bruce founded The Shmoo Group (TSG), an ad-hoc group of security professionals scattered throughout the world. Bruce's interests include wireless security, large-scale network architectures, open-source software assistance, and promotion of secure software engineering.

Preston Norvell is a project and security engineer for Mercury Data Group, a large IT consulting firm serving the state of Alaska and locations abroad. Preston was educated in computer science at the University of Alaska Fairbanks and has since been a senior engineer at various IT firms in the state. A member of The Shmoo Group since 1999, Preston is the progenitor of TSG's MacSecurity.org web site. Preston's interests and experience includes open-source software, network design, heterogeneous systems integration, network and systems security, and practical bioinformatics.

Brian Wotring is an experienced software engineer with an intense devotion to software security. Brian studied computer science and mathematics at both the University of Alaska and the University of Louisiana.

As a long-standing member of The Shmoo Group of security and privacy professionals, Brian has an interest in open-source software development, secure programming engineering, and file-integrity systems. He is responsible for the development of Osiris, a file-integrity management application. With the help of The Shmoo Group, Osiris is on the road to becoming a host-based intrusion detection system. Brian also founded and maintains knowngoods.org, an online database of file signatures for numerous operating systems.

About the Technical Reviewers

These reviewers contributed their considerable hands-on expertise to the entire development process for *Mac OS X Security*. As the book was being written, these dedicated professionals reviewed all the material for technical content, organization, and flow. Their feedback was critical to ensuring that *Mac OS X Security* fits our reader's need for the highest-quality technical information.

John Viega is an internationally recognized expert on software security. He has co-authored three books in the field, including *Building Secure Software* (Addison-Wesley, 2001), *Network Security with OpenSSL* (O'Reilly, 2002), and *Secure C Programming Cookbook* (O'Reilly, 2003). John is the founder and Chief Scientist of Secure Software (www.securesoftware.com), an Adjunct Professor at Virginia Tech, and a Senior Research Scientist at the Cyberspace Security Policy and Research Institute. He also serves on the board of directors for the Secure Trusted OS Consortium (STOS).

Roland Miller is an information security manager at a large research university. His background includes business management as well as MS and BS degrees in Mechanical Engineering. He has significant experience with Windows NT/2000 and Mac OS/Mac OS X in terms of security, integration, and support. He currently holds CISSP, GCFA, GSEC, MCSE, and MCP+I certifications.

Acknowledgments

I would first like to thank my wife, Heidi, and two children, Terran and Robert. They gave me the time and support needed to research and write this book. Without them, I never would have made it. I would like to thank the members of The Shmoo Group. You guys and gals have been the foundation for much of my technical work for the last few years. Also, the team at New Riders has been great. Thanks to Linda Bump and Chris Zahn for their outstanding effort in getting this book published, as well as our technical reviewers John Viega and Roland Miller.

My first introduction to OS X was at a place called FortNOCS where I worked with Preston and Brian. We spent many a long day porting standard UNIX applications to OS X Server. OS X Server had just been released and Client was still a year away. We learned a lot about the innards of OS X and how great an operating system it was shaping up to be. Preston and Brian taught me an incredible amount about the history of Macs, the hardware, and the future of OS X. The knowledge they instilled in me has been invaluable in my continuing experience with OS X. I am lucky to have them as teachers, co-authors, and friends. Thanks, guys.

—Bruce Potter

I would like to thank my friends, family, and co-workers for their patience and understanding during this process—it was more appreciated than I ever conveyed. I would like to thank a junior high school friend named Steve Ball, wherever he is, for introducing me to Macintoshes. Thanks also go out to my grandmother, Peggy Linder, for giving me my first Mac, a Macintosh XL (which actually ran Xenix, but that is another story for another day). And then there are thanks to my parents who gave me my first modern Mac (with a ginchy new PowerPC in it) as well as doing all that other stuff great parents do.

I would especially like to thank my co-writers for their work and their patience. I met Bruce many moons ago at the university in Fairbanks, Alaska. He was responsible for me getting my first real IT job, as well as getting me interested in security when we were reunited a couple years later at a company named FortNOCS. It was there that I was also introduced to Brian, a momentous occasion of small proportions that I am sure he rues to this day. They are both good friends and comrades-at-arms, and I can think of no two people with whom I would rather write a book.

Last, I would like to thank the New Riders crew (Linda Bump and Chris Zahn), and our technical editors (John Viega and Roland Miller) for their patience, guidance, and expertise—without their help this book would not be what it is.

—Preston Norvell

First, I would like to thank my wonderful wife, Kaleigh. My part in this book would not have been possible without her patience and support over the last months.

I would like to thank The Shmoo Group for all that I have learned from them over the years. I want to thank Paul Holman for being such a faithful friend and mentor, and for turning me on to OpenStep when I was in school.

Thanks to Bruce and Preston for being excellent technical partners and co-authors. Working on this book reminded me how much I have learned as a result of us having been co-workers, and co-conspirators to

various projects. Thank you both for your friendship, and for the technical adventures we've had over the years.

Many thanks to New Riders, specifically Chris Zahn and Linda Bump for all their efforts in making this book come together. Thanks to Roland Miller for his role as technical reviewer and for helping out with various Mac OS X issues.

Finally, I would like to personally thank John Viega for his expertise and insight, as a technical editor for this book, and as a contributor to the field of computer security. This book has truly benefited from his time and input.

—Brian Wotring

Tell Us What You Think

As the reader of this book, you are the most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As the senior Acquisitions Editor for this book, I welcome your comments. You can fax, email, or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger. When you write, please be sure to include this book's title, ISBN, and author, as well as your name and phone or fax number. I will carefully review your comments and share them with the author and editors who worked on the book.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of email I receive, I might not be able to reply to every message.

Fax:	317-581-4663
Email:	linda.bump@newriders.com
Mail:	Linda Anne Bump Acquisitions Editor New Riders Publishing 201 West 103rd Street Indianapolis, IN 46290 USA

Introduction

This book is about security. Specifically, it is about understanding security issues with Mac OS X. From the basic framework of the operating system, to host-based security, to integration into an enterprise network, this book covers it all.

Mac OS X is a powerful operating system. It contains new security features that go above and beyond previous versions of Mac OS. There are keychains to store passwords. Disk volumes can be encrypted so other users cannot read your data. Permissions on files and directories can be controlled on a user and group basis. It is interoperable with more industry standards and operating systems than previous versions of Mac OS ever aspired to. With NetInfo, large-scale users and resource management is reality. Mac OS X systems can be integrated into enterprise directory services, such as Active Directory and Apple's own Open Directory for management of users and resources.

Mac OS X is also more dangerous to use than previous Apple operating systems if not installed and configured correctly. Without understanding how various configuration files and commands alter the state of the machine, a user can quickly break down any security barriers that existed in the default install and leave themselves open to attack.

We will not only cover the tools and security issues, but also provide practical application and configurations where needed. By the end of this book, you will understand how to defend and audit a Mac OS X installation and how to avoid common mistakes that can expose you to security risks.

Organization and Content

We have divided this book into five major parts. In the following sections, we provide a brief overview of each part that makes up this book.

Part I: The Basics

Part I begins with an overview of security and the fundamentals of Mac OS X security. Chapter 1, "Security Foundations," covers some basic risks and the user/group model. Chapter 2, "Installation," highlights the issues surrounding various installations of the operating system, including guides for both the client and server versions of Mac OS X.

Part II: System Security

Part II focuses on Mac OS X on the workstation. When used as a workstation, Mac OS X has specific security considerations that need to be addressed on a per-user and per-application basis. Chapter 3, "Mac OS X Client General Security Practices," covers general practices, such as dual booting and patching the operating system. Chapter 4, "What Is This UNIX Thing?," introduces the UNIX-layer by detailing file permissions and the security risks associated with a UNIX operating system. Many applications that ship with Mac OS X have their own particular security domains. Chapter 5, "User Applications," covers application-level security, including risks and solutions for securing commonly used applications.

Part III: Network Security

Along with the powerful UNIX underpinnings comes a host of new networking capabilities. These are addressed in Part III. Chapter 6, "Internet Services," explores the major facets of Mac OS X's network services, their peculiarities, and how they can be deployed in a secure fashion. Chapter 7, "File Sharing," deals with issues related to file sharing, including NFS, AFS, SMB, and WebDAV services. Chapter 8, "Network Services," focuses on the tools and configuration options that can be used to defend a Mac OS X system from network attacks and reduce network vulnerabilities. This includes topics such as VPNs, firewalls, and wireless security.

Part IV: Enterprise Security

Part IV of this book addresses Mac OS X security on a larger scale. Apple is positioning Mac OS X Server as the keystone in their enterprise architecture. Maintaining an enterprise full of workstations and servers can be a daunting task. This section covers the security issues that administrators encounter when using Mac OS X Server as the core of their infrastructure. Chapter 9, "Enterprise Host Configuration," includes Kerberos Integration, Rendezvous, and WebDAV management. Chapter 10, "Directory Services," explores Mac OS X's capability to integrate into enterprise directory services. The three directory services covered in this chapter are Active Directory, Open Directory, and NetInfo.

Part V: Auditing and Forensics

Part V deals primarily with verifying the integrity of a Mac OS X-based infrastructure, and what to do when

a system is compromised. No matter how secure a Mac OS X installation is, it may be broken into over time. Without understanding how to audit hosts and respond to attacks, all the previous sections in this book are near useless. Auditing tends to be forgotten in the realm of computer security. Chapter 11, "Auditing," explains the built in logging facilities of Mac OS X, how to set up logging correctly, and how to monitor logs. Chapter 12, "Forensics," explores forensic solutions for Mac OS X. This includes host integrity management and post-mortem analysis tools. Finally, Chapter 13, "Incident Response," covers incident recognition, response, and prevention issues from both a user and an administrative perspective.

Part VI: Appendixes

For information that did not fit well in any of the chapters, we have provided appendixes: Appendix A, "SUID and SGID Files," Appendix B, "Common Data Security Architecture," and Appendix C, "Further Reading."

PREVIOUS NEXT

Target Audience

This book is aimed at intermediate to advanced Mac OS X users. It was our goal to make this book something that anyone from a home user to an administrator would find valuable.

We assume the reader has a working knowledge of Mac OS X. Due to the technical variety of this audience, some of the material assumes a knowledge of basic UNIX commands. For readers new to UNIX, we recommend the book *Learning UNIX for Mac OS X*, 2nd Edition, by Dave Taylor and Brian Jepson (O'Reilly & Associates).

Mac OS X Security may also be of interest to advanced users of other operating systems such as Windows or Linux, system administrators, and security administrators. Due to the UNIX core, Mac OS X is now a viable option to deploy in large-scale desktop and server environments. Administrators need to understand the innermost details of the operating system to be able to secure hundreds of hosts at a time.

Additionally, we have set up a web site containing resources and information that was not practical to include in this book. This site also contains updated information, an errata listing, links to applications, and references related to the material mentioned throughout the text. Check it out at

http://www.macsecurity.org/osx-book

Send email to

osx-book@macsecurity.org

Code Convention Used in This Book

We've designed Mac OS X Security to be easy to use. One thing we'd like to point out is the use of code continuation characters in code lines. When code lines wrap to a second or third line, you will see a \ at the end of the first line, and -> at the beginning of the runover lines:

```
bash-2.05a$ sudo osiris -f /var/db/osiris/configs/daily.conf -o /var/db/osiris/base.osi

bash-2.05a$ mactime -z MST7MDT -b seizure-copy1.mac > seizure-copy1.timeline
```

Part I: The Basics

Chapter 1. Security Foundations

"The loftier the building, the deeper must the foundation be laid."

—Thomas Kempis

The most recent version of Mac OS is a multitasking, multithreaded, multiuser, and multiprocessing operating system. Yesterday, Macintosh users were using a relatively simplistic system, while today they are using a powerful UNIX-based operating system that may become a prime target for attackers. The security knowledge of an average Mac user is currently very limited; the historical security of the Mac OS operating system and the focus on ease of use conspire to make it so.

Mac OS X contains many security features, but without an understanding of what those features are, and how to put them in place, users can quickly leave themselves open to attack. This book is about understanding the risks, as well as the procedures and tools to reduce those risks.

We begin with an overview of the risks, why these risks are real, and what technologies exist to address those risks. Finally, we explore the basics of the UNIX security model as it applies to Mac OS X. The material covered in this chapter provides a basis to aid in the understanding of the remainder of the material covered in this book. Those with strong UNIX backgrounds might be tempted to skip over this chapter; however, many peculiarities of Mac OS X are covered, so you are encouraged to stick around.