Foundations of Mac OS X Leopard Security

Charles S. Edge, Jr., William Barker, and Zack Smith

Apress®

FOUNDATIONS OF MAC OS X LEOPARD SECURITY

ISBN-13 (pbk): 978-1-59059-989-1

ISBN-10 (pbk): 1-59059-989-6

ISBN-13 (electronic): 978-1-4302-0646-0

ISBN-10 (electronic): 1-4302-0646-2

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Lead Editor: Jeffrey Pepper
Technical Reviewers: Mike Lee, Frank Pohlmann
Editorial Board: Clay Andres, Steve Anglin, Ewan Buckingham, Tony Campbell, Gary Cornell, Jonathan Gennick, Matthew Moodie, Joseph Ottinger, Jeffrey Pepper, Frank Pohlmann, Ben Renow-Clarke, Dominic Shakeshaft, Matt Wade, Tom Welsh
Project Manager: Candace English
Copy Editor: Kim Wimpsett
Associate Production Director: Kari Brooks-Copony
Senior Production Editor: Laura Cheu
Compositor: Susan Glinert Stevens
Proofreader: Nancy Bell
Indexer: Julie Grady
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail orders-ny@springer-sbm.com, or visit http://www.springeronline.com.

For information on translations, please contact Apress directly at 2855 Telegraph Avenue, Suite 600, Berkeley, CA 94705. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit http://www.apress.com.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book is dedicated to my loving wife, Lisa.
—Charles

To my family and friends, who incessantly inspire me to follow my dreams.
—William

Contents at a Glance

PART 1 ■■■ The Big Picture

PART 2 ■■■ Security Essentials

PART 3 ■■■ Network Security

PART 4 ■■■ Sharing

PART 5 ■■■ Workplace Security

Contents

PART 1 ■■■ The Big Picture

PART 2 Security Essentials

PART 3 ■■■ Network Security

PART 4 ■■■ Sharing

PART 5 Workplace Security

About the Authors

CHARLES EDGE has been working with Apple products since he was a child. Professionally, Charles started with the Mac OS and Apple server offerings in 1999 after years of working with various flavors of Unix. Charles began his consulting career working with Support Technologies and Andersen Consulting. In 2000, he found a new home at 318, a consulting firm in Santa Monica, California, which is now the largest Mac consultancy in the country. At 318, Charles leads a team of more than 40 engineers and has worked with network architecture, security, and storage for various vertical and horizontal markets. Charles has spoken at a variety of conferences including DefCon, Black Hat, LinuxWorld, Macworld, and the WorldWide Developers Conference. Charles' first book, *Mac Tiger Server Little Black Book*, can be purchased through Paraglyph Press. Charles recently hung up his surfboard and moved to Minneapolis, Minnesota, with his wife, Lisa. Charles can be contacted at `krypted@mac.com`.

WILLIAM BARKER is a technical consultant at 318 and a freelance writer. He has a penchant for all things Web 2.0 related and is eagerly anticipating the day he can wash his dishes and take out the trash online. His web site, `techiestravel.com`, is a hobby haven for two of his passions, technology and travel. He also wears a musician hat from time to time, making music: DJing, playing guitar, playing piano, and mixing CDs for friends. He lives in Venice, California, with his trusty automobile, Lucille.

ZACK SMITH has been working as an IT consultant his entire adult life. He has consulted for insurance companies, entertainment companies, medical organizations, and governmental agencies. Zack is an Apple Certified Trainer and has taught at Apple and various market centers in Boston, Virginia, Los Angeles, and Cupertino. As a certified instructor, Zack has taught Apple's Security Best Practices class, as well as many other system administrator–level classes (such as Mac OS X Deployment and Mac OS X Directory Services). Zack has been a speaker at Macworld San Francisco as well as many other smaller venues such as IT user groups. Zack is also the author of a set of open source IT administration software and scripts and has long-term plans of being a full-time Objective C developer. When not attending IT and security conferences or traveling for work at 318, Zack can be found in Portland, Oregon, with his partner in crime, Anna, and dog, Watson.

About the Technical Reviewer

MIKE LEE, the world's toughest programmer, has been bending computers to his will since the mid-90s. Having recently retired as majordomo of Delicious Monster Software, he's now working at United Lemur, a charity-driven software company dedicated to raising money and awareness for Madagascar and the world's few remaining lemurs. Mike and his wife are originally from Honolulu but currently live in Seattle, where they are raising two cats. Mike's hobbies include weightlifting, single malts, and fire. Mike can be contacted at `mike@unitedlemur.org`.

Acknowledgments

I'd like to thank all the folks at Apple for the hard work they have put into the various flavors of OS X and into educating the Mac community on their fantastic product, in particular, Joel Rennich, Schoun Regan, Josh Wisenbaker, Greg Smith, JD Mankovsky, David Winter, Stale Bjorndal, Eric Senf, Cawan Starks, Martin Libich, and a short list of others who have helped me through the years! This includes the late Michael Bartosh, who is sorely missed on many fronts.

Thanks are also in order to the crew at 318 for their hard work, especially Kevin Klein. Without you guys I never would have been able to take the time to complete this book: David, Tim, Thomas, Beau, Zack, Kevin, Kevin, William, Joel, Robert, Jordan, Susie, Dan, Phil, Max, Daniel, Adrian, John, John, Jon, Marc, Monica, Karl, Chris, Cade, Christian, Eli, Drake, Erin, Ehren, Kennon, Theresa, Tony, and everyone else.

Also thanks to the fine staff at Apress for turning this book into something to be proud of: Jeffrey Pepper, Candace English, Kim Wimpsett, Tina Nielsen, Steve Anglin, and the myriad of others whose hard work went into this title. Thanks also to the technical reviewer, Mike Lee, and to my coauthors, Zack and William.

I also have to thank the organizers of SANS, DefCon, BlackHat, LayerOne, and the other security conferences and those in the white/gray hat and InfoSec communities for bringing to light many vulnerabilities before they are discovered by others with a flair for exploitation. Finally, a huge thanks goes out to the open source community. It is on the shoulders of these giants that we all sit!

Charles S. Edge, Jr.

Many thanks are in order for making this dream a reality. I'd be remiss if I didn't thank my coauthor Charles Edge who brought me into this crazy experience in the first place. Thank you to everyone at Apress (Candace, Laura, Mike, Kim, and all the others) for their tireless work and dedication to this book. The development team at Apple should be acknowledged for their constant desire to improve and reinvent a product that continues to amaze novices and experts alike. My parents deserve a huge thank you for introducing me to the wonders of reading and computer technology at a very early age. A heartfelt thanks goes to my good friend Adam, who took a chance at giving me my first paid writing job and is a constant inspiration to my craft. Last but certainly not least, this book is inspired by the technical writers of the world. It is an unsung art to write technically, and the attention to detail that those who write books covering technical materials must provide is truly staggering. Because of their experimentation, we learn how to make our lives easier and more enjoyable.

William Barker

Introduction

A common misconception in the Mac community is that the Mac is more secure than any other operating system on the market. Although this might be true in most side-by-side analyses of security features right out of the box, what this isn't taking into account is that security tends to get overlooked once the machine starts to be configured for its true purposes. For example, when sharing is enabled or remote control applications are installed, then a variety of security threats are often established—no matter what the platform is.

In the security sector, the *principle of least privilege* is a philosophy that security professionals abide by when determining security policies. This principle states that if you want to be secure, you need to give every component of your network the absolute minimum permissions required to do its job. But what are those permissions? What are the factors that need to be determined when making that decision? No two networks are the same; therefore, it's certainly not a decision that can be made for you. It's something you will need to decide for yourself based on what kinds of policies are implemented to deal with information technology security.

Security Beginnings: Policies

Security in a larger organization starts with a security policy. When looking to develop security policies, it is important that the higher-level decision makers in the organization work hand in hand with the IT team to develop their policies and security policy frameworks. A security policy, at a minimum, should define the tools used on a network for security, the appropriate behavior of employees and network users, the procedures for dealing with incidents, and the trust levels within the network.

The reason policies become such an integral part of establishing security in a larger environment is that you must be secure but also be practical about how you approach security in an organization. Security can be an impediment to productivity, both for support and for nonsupport personnel. People may have different views about levels of security and how to enforce it. A comprehensive security policy makes sure everyone is on the same page and that the cost vs. protection paradigm that IT departments follow are in line with the business logic of the organization.

On small networks, such as your network at home, you may have a loose security policy that states you will occasionally run security updates and follow a few of the safeguards outlined in this book. The smaller a network environment, the less likely security is going to be taken seriously. However, for larger environments with much more valuable data to protect, the concern for security should not be so flippant. For example, the Health Insurance Portability and Accountability Act (HIPAA) authorizes criminal penalties of up to $250,000 and/or 10 years imprisonment per violation of security standards for patient health information. The Gramm-Leach-Bliley Act establishes financial institution standards for safeguarding customer information and imposes penalties of up to $100,000 per violation.

Everyone in an organization should be concerned about security policies because everyone is affected to some extent. Users are often affected the most, because policies often consist of a set of rules that regulate their behavior, sometimes making it more difficult for them to accomplish their tasks throughout their day. The IT staff should also be consulted and brought into the decision-making process since they will be required to implement and comply with these policies, while making sure that the policies are realistic given the budget available. In addition, you must notify people in advance of the development of the policy. You should contact members of the IT, management, and legal departments as well as a random sampling of users in your environment. The size of your policy development will be determined by the scope of the policy and the size of your organization. Larger policies may require many people to be involved in the policy development. Smaller policies may require participation by only one or two people within the organization.

As an example, a restrictive policy that requires all wireless users to use a RADIUS server would incur IT costs not only from the initial install but also with the installs and configurations necessary to set up the RADIUS clients on each of the workstations. A more secure RADIUS server would also cause additional labor over other less secure protocols such as WEP. You also need to consider IT budgeting and staffing downtime.

When developing your actual policy, keep the scope limited to what is technically enforceable and easy to understand, while protecting the productivity of your users. Policies should also contain the reasons a policy is needed and cover the contacts and responsibilities of each user. When writing your policy, discuss how policy violations will be handled and why each item in the policy is required. Allow for changes in the policies as things evolve in the organization.

Keep the culture of your organization in mind when writing your security policy. Overly restrictive policies may cause users to be more likely to ignore them. Staff and management alike must commit to the policies. You can often find examples of acceptable use policies in prepackaged policies on the Internet and then customize them to fulfill your organization's needs.

A Word About Network Images

Whether you are a home user or a corporate network administrator, the overall security policy of your network will definitely be broken down into how your computers will be set up on the network. For smaller environments, this means setting up your pilot system exactly the way you want it and then making an image of the setup. If anything were to happen to a machine on your network (intrusion or virus activity, for example), you wouldn't need to redo everything from scratch. If you're in a larger, more corporate environment, then you'll create an image and deploy it to hundreds or thousands of systems using NetInstall, Casper Suite, LanDESK, or a variety of other tools that you may or may not have experience with.

Risk Management

By the end of this book, we hope you will realize that if a computer is plugged into a network, it cannot be absolutely guaranteed secure. In a networked world, it is not likely that you will be able to remove all of the possible threats from any networked computing environment. To compile an appropriate risk strategy, you must first understand the risks applicable in your specific environment. Risk management involves making decisions about whether assessed risks are sufficient enough to present a concern and the appropriate means for controlling a significant risk to your environment. From there, it is important to evaluate and select alternative responses to these risks. The selection process requires you to consider the severity of the threat.

For example, a home user would likely not be concerned with security threats and bugs available for the Open Directory services of Mac OS X Server. However, in larger environments running Open Directory, it would be important to consider these risks.

Risk management not only involves external security threats but also includes fault tolerance and backup. Accidentally deleting files from systems is a common and real threat to a networked environment.

For larger environments with a multitude of systems requiring risk management, a risk management framework may be needed. The risk management framework is a description of streams of accountability and reporting that will support the risk management process for the overall environment, extending beyond information technology assets and into other areas of the organization. If you are managing various systems for a large organization, it is likely there is a risk management framework and that the architecture and computer policies you implement are in accordance with the framework.

All too often, when looking at examples of risk management policies that have been implemented in enterprise environments, many Mac administrators will cite specific items in the policies as “not pertaining” to their environment. This is typically not the case, because best practices are best practices. There is a reason that organizations practice good security, and as the popularity of Mac based network environments grows, it is important that administrators learn from others who have managed these enterprise-class environments.

As mentioned earlier, managing IT risk is a key component of governmental regulations. Organizations that fall under the requirements of Sarbanes-Oxley, HIPPA, or the Gramm-Leach-Bliley Act need to remain in compliance or risk large fines and/or imprisonment. Auditing for compliance should be performed on a regular basis, with compliance documentation ready and available to auditors.

Defining what is an acceptable risk is not something that we, the authors of this book, can decide. Many factors determine what is an acceptable risk. It is really up to you, the network administrator, to be informed about what those risks are so that you can make an informed decision. We will discuss options and settings for building out secure systems and a secure networked environment for your system. However, many of the settings we encourage you to use might impact your network or system in ways that are not acceptable to your workflow. When this happens, a choice must be made between usability and performance. Stay as close to the principle of least privilege as much as possible, keeping in mind that you still need to be able to do your job.

How This Book Is Organized

The first goal of this book is to help you build a secure image, be it at home or in the office, and then secure the environment in which the image will be used. This will involve the various options with various security ramifications, but it will also involve the network, the sharing aspects of the system, servers, and finally, if something drastic were to happen, the forensic analysis that would need to occur.

Another goal of this book is to provide you with the things to tell users not to do. Adding items to enforce your policy and security measures will help you make your network, Mac, or server like a castle, with various levels of security, developed in a thoughtful manner. To help with this tiered approach, we've broken the book down into five parts.

Part 1: The Big Picture

First, an introduction to the world of security on the Mac comprises Part 1:

Chapter 1, "Security Quick-Start": If you have time to read only one chapter, this is the chapter for you. In this chapter, we cover using the GUI tools provided by Apple to provide a more secure environment and the best practices for deploying them. We give recommendations and explain how to use these various features and when they should be used. We also outline the risks and strategies in many of their deployments.

Chapter 2, "Security Fundamentals": In this chapter, we define many of the common risks to users and computers. We then focus on many of the common security principles used when securing an operating system and the network environment. This chapter is a birds'-eye view into the complex world of information security.

Chapter 3, "Securing User Accounts": Mac OS X is a multiuser operating system. One of the most important security measures is to understand the accounts on your system and when you are escalating privileges for accounts. This chapter explains how to properly secure these users and groups.

Part 2: Security Essentials

Part 2 gets down to some of the essential elements of security on a Mac:

Chapter 4, "Malware Security: Combating Viruses, Worms, and Root Kits": Viruses, spyware, and root kits are at the top of the list of security concerns for Windows users. However, Mac users are not immune. In this chapter, we go into the various methods that can be used to protect Mac systems against these and other forms of malware.

Chapter 5, "Securing Web Browsers and E-mail": Safari, Firefox, Internet Explorer, Mail.app, and Entourage—with all these programs to manage, how do you lock them all down appropriately? In this chapter, we discuss cookies, Internet history, and browser preferences and when you should customize these settings. We also give some tips for third-party solutions for protecting your privacy. In addition, this chapter provides readers with best security practices for the mail clients that they likely spend much of their time using.

Chapter 6, "Reviewing Logs and Monitoring": What good are logs if they aren't reviewed? In this chapter, we discuss what logs should be reviewed and what is stored in each file. We then move on to various monitoring techniques and applications and the most secure ways to deploy them in typical environments.

Part 3: Network Security

Part 3 describes how you secure a Mac network:

Chapter 7, "Securing Network Traffic": As useful as securing the operating system is, securing the network backbone is a large component of the overall security picture. In this chapter, we explore some of the techniques and concepts behind securing the network infrastructure. This includes the common switches, hubs, and firewalls used in Mac environments and the features you may have noticed but never thought to tinker with. We also cover how to stop some of the annoying issues that pop up on networks because of unauthorized (and often accidental) user behavior.

Chapter 8, "Setting Up the Mac OS X Firewall": The firewall option in Mac OS X is just a collection of check boxes. Or is it? We discuss using and securing the Mac OS X software firewall, and we go into further detail on configuring this option from the command line. We also discuss some of the other commands that, rather than block traffic, allow an administrator to actually shape the traffic, implementing rules for how traffic is handled, and mitigate the effects that DoS attacks can have on the operating system.

Chapter 9, "Securing a Wireless Network": Wireless networking is perhaps one of the most insecure things that users tend to implement themselves. In this chapter, we cover securing wireless networks, and then, to emphasize how critical wireless security is (and how easy it is to subvert it if done improperly), we move on to some of the methods used to exploit wireless networks.

Part 4: Sharing

File Sharing needs a section all to itself. Files are what hackers are after, and securing them should be a top priority in any environment. Part 4 covers the following:

Chapter 10, "File Services": What is a permission model, and why do you need to know what it is, when all you want to do is allow people access to some of the files on my computer? Knowing the strategies involved in assigning file permissions is one of the most intrinsic security aspects of a shared storage environment. It is also important to understand the specific security risks and how to mitigate them for each protocol used, including AFP, FTP, NFS, and SMB, which are all covered in this chapter.

Chapter 11, "Web Site Security": Apache is quite possibly the most common web server running on the *nix platform. Entire books are dedicated to explaining how to lock down this critical service. In this chapter, we focus on the most important ways to lock down the service and some Apple-centric items of Apache not usually found in discussions about Apache on the *nix platform. We also provide you with other resources to look to if you require further security for your web server.

Chapter 12, "Remote Connectivity": One of the most dangerous aspects of administration is the exposure of the very tools you use to access systems remotely. Many of these programs do not always need to be running and can be further secured from their default settings. In this chapter, we cover many of the methods for protecting these services and some of the ways that vendors should change their default settings to make them more secure. We also cover some of the ways you can secure these tools, and we help administrators make choices about how to best implement remote administration utilities to counteract these shortcomings.

Chapter 13, "Server Security": Mac OS X Server is very much like Mac OS X Client, without many of the bells and whistles and with a more optimized system for sharing resources. This is true with many server-based operating systems. Because a Mac OS X server fills a different role in a networked environment, it should be treated differently from Mac OS X Client. For this reason, we cover many of the security options that are available as well as those that are crucial to securing Mac OS X Server. We also cover many of the security options from Mac OS X that should specifically not be used in Mac OS X Server.

Included with server security is directory services, which are critical to expanding technology infrastructures. By interconnecting all the hosts of a network, you are able to better control the settings and accounts on systems. In this chapter, we also focus on the ways to securely deploy Mac OS X clients to various directory services and point out the items to ask for (if you are in a larger network infrastructure) or to set up in order to help make the directory service environment as secure as possible.

Part 5: Workplace Security

How secure is your work environment's network? This part explores security as it pertains to environments with multiple Mac computers connected on a network:

Chapter 14, "Network Scanning, Intrusion Detection, and Intrusion Prevention Tools": Host-based intrusion detection systems (IDS) are quickly becoming a standard for offering signature-based and anomaly-based detection of attacks. Some of these tools allow for augmenting the operating system settings to further secure the hosts on which they run. In this chapter, we provide a best practices discussion for deploying and using IDSs. We also cover the various attacks that have been developed over the past few years against IDS systems and explore add-ons for IDSs that provide rich aggregated data about the systems.

Chapter 15, "Backup and Fault Tolerance": If you don't have a backup plan now, then you will after you read this chapter. Backups are the last line of defense in a security environment. Backups are critical and should be provided in tiers. In this chapter, we describe some of the strategies for going about implementing a backup plan, from choosing the right software package to properly implementing it. We also cover some of the more common techniques for providing fault-tolerant services and the security risks that can be introduced by doing so.

Chapter 16, "Forensics": What do you do when your systems are compromised? What happens after the attack? In this chapter, we cover the basics of computer forensics and how a user can be their own digital sleuth. The goal is not to have you testifying in court on large-scale network attacks but instead to help first responders get comfortable with safely imaging Mac systems for investigations without contaminating evidence.

Appendixes

The following are the appendixes:

Appendix A, "Xsan Security": Here we provide tips on securing your Xsan.

Appendix B, "Acceptable Use Policy": This appendix contains an acceptable use policy from the SANS Institute that has been reprinted here with their consent.

Appendix C, "Secure Development": Here we give a brief rundown of Apple's development architecture.

Appendix D, "Introduction to Cryptography": In this appendix, we give a brief history of cryptography and look at some of the protocols used today and how they came about.