Hardening Apache

TONY MOBILY

Apress™

Hardening Apache

ISBN: 1-59059-378-2

Printed and bound in the United States of America 10987654321

Lead Editor: Jim Sumser

Technical Reviewers: Ken Coar and Jonathan Hassell

Editorial Board: Steve Anglin, Dan Appleman, Gary Cornell, James Cox, Tony Davis, John Franklin, Chris Mills, Steve Rycroft, Dominic Shakeshaft, Julian Skinner, Jim Sumser, Karen Watterson, Gavin Wray, John Zukowski

Project Manager: Nate McFadden

Copy Manager: Nicole LeClerc

Copy Editor: Brian MacDonald

Production Manager: Kari Brooks

Production Editor: Kelly Winquist

Compositor: Molly Sharp, ContentWorks

Proofreader: Liz Welch

Indexer: Valerie Hanes Perry

Artist: Kinetic Publishing Services, LLC

Cover Designer: Kurt Krames

Manufacturing Manager: Tom Debolski

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY, 10010 and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, email orders@springer-ny.com, or visit http://www.springer-ny.com. Outside the United States: fax +49 6221 345229, email orders@springer.de, or visit http://www.springer.de.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, email info@apress.com, or visit http://www.apress.com.

The source code for this book is available to readers at http://www.apress.com in the Downloads section.

Foreword

Congratulations! You have before you a book whose time has more than come.

More and more attention has been forcibly drawn to the issues of computer and information security. Only a few years ago, it was an afterthought for just about everybody connected with computers or networks; now it is an exceedingly rare week that passes without at least one alert of a security vulnerability affecting tens of thousands of users.

Two factors (at least!) have contributed to this explosive growth of awareness and concern. One is the increasing ubiquity of computer access; more and more individuals must use a computer as part of their daily jobs, and increasing numbers of families have computers at home. And almost every single one of these computers has the potential, realized or not, of being connected to a network that includes hundreds to millions of others.

Another major contributing factor is the ever-expanding demand for more and more functionality and capability. Not only does meeting this demand require faster hardware; it also requires more complicated software. The faster hardware and network connections makes certain attack forms (such as password bashing) more viable, and the increasing complexity of the software inevitably introduces more nooks and crannies in which some sort of oversight or bug might hide.

What does all this have to do with *Hardening Apache*? The Apache Web server is one of those bits of software that has become increasingly involved and esoteric as it has grown to meet the demands of its users and developers for more functionality. Combine the potential for security vulnerabilities with the pervasiveness of the package (which at the time of this writing drives more than thirty million web sites—over two thirds of the Web!) and you have a very attractive target for crackers.

In addition to the complexity of the base Apache `httpd` package, its design permits—nay, encourages—third-party vendors to extend its functionality with their own special-purpose code. So regardless of the security robustness of Apache itself (and it's pretty robust) some less well-scrutinized after-market package may introduce vulnerabilities.

Despite the foregoing and the popularity of the Apache web server, there is a surprising dearth of authoritative and complete documents providing instructions for making an Apache installation as secure as possible.

Enter *Hardening Apache*. In it, Tony Mobily takes you from obtaining the software and verifying that no one has tampered with it, through installing and configuring it, to covering most of the attack forms that have been mounted against it. In each case, he describes what the issue is, how it works, whether it

has been addressed by the Apache developers (so you can tell if upgrading will correct it), and various actions you can take to prevent penetration.

Software is a moving target, and documenting it is a difficult and never-ending task. So in addition to giving you information as current as possible as of the time of this writing, *Hardening Apache* also includes pointers to online sources and mailing lists that you can use to keep up with the latest news, views, and clues concerning vulnerabilities and attack forms.

As I said: a book whose time has more than come.

Ken Coar,
Apache Software Foundation,
February 2004