Extracted from:

Practical Security

Simple Practices for Defending Your Systems

The Pragmatic Bookshelf

Raleigh, North Carolina

The Pragmatic Programmers

Pragmatic exPress

Practical Security

Simple Practices for Defending Your Systems

Roman Zabicki
edited by Adaobi Obi Tulton

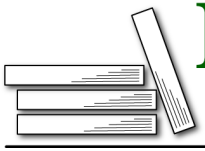
Practical Security

Simple Practices for Defending Your Systems

Roman Zabicki

The Pragmatic Bookshelf

Raleigh, North Carolina



Our Pragmatic books, screencasts, and audio books can help you and your team create better software and have more fun. Visit us at *https://pragprog.com*.

The team that produced this book includes:

Publisher: Andy Hunt
VP of Operations: Janet Furlow
Managing Editor: Susan Conant
Development Editor: Adaobi Obi Tulton
Copy Editor: Molly McBeath
Layout: Gilson Graphics

For sales, volume licensing, and support, please contact *support@pragprog.com*.

For international rights, please contact *rights@pragprog.com*.

ISBN-13: 978-1-68050-634-1
Book version: P1.0—February 2019

To Marnie

Thanks for all the geek time

Introduction

It seems like hardly a week goes by without a high-profile computer breach. Why do these happen? How can you prevent them? This book doesn't have all the answers, but it does outline practices that make life harder for attackers and that help tide you over until you get a full-time security team in place.

This book is about getting the security basics right when you're starting out (or if you've been at it a while but haven't had guidance). There's no getting around the need for bringing on full-time security staff and outside security consultants as your organization gets more mature. Lots of complex security decisions require the judgment of a professional who has the full context of your particular situation. But if you have the basics taken care of, you'll free up the experts to take on harder problems and you'll get more out of them.

When you first bring in security consultants, you may only have a budget for one engagement per year. That's your one shot to learn from these experts. They'll happily report on the kinds of things outlined in this book. But that will eat up the time allocated for the engagement. You'll have spent your budget, and you'll have to wait another year before you get a chance to learn anything else from them. Don't spend a year and tens of thousands of dollars to learn the things that you could learn in a week by reading this book.

Who Is This Book For?

This book is for developers, admins, team leads, architects, technology generalists, and all others who stand guard against the things that go bump in the network. It's particularly for those who work in organizations that don't have dedicated security staff or don't have much interaction with dedicated security staff. If you thought that a couple of those job titles could apply to you, this book is for you. Sometimes these kinds of organizations are startups. Sometimes they're software development teams in large, well-established

companies who have been left on their own to determine their own security posture alongside their regular day job of building useful software systems.

What's in This Book

This book covers five basic practices to improve your security posture.

Start with Chapter 1, *Patching*, on page ?. What happens when a serious vulnerability makes headlines? You need to quickly and authoritatively discover whether you use that software and then patch it if needed. Hopefully you have this capability today. If not, you can build up the capability to respond to this scenario now, when you're not rushed, when you can plan, prioritize, and test the work just like any other engineering work. Or you can wait until it's an emergency.

Next, you'll explore some basic software vulnerabilities in Chapter 2, *Vulnerabilities*, on page ?. You'll see how they work, how to prevent them, and, in some cases, how to make attempts to exploit them more detectable. You'll also learn about some common misconfigurations that can take otherwise secure software and open it up to attack.

You've probably heard the advice "Never write your own crypto." In Chapter 3, *Cryptography*, on page ?, you'll find out why this is good advice. You'll also discover some cryptography libraries you can use instead.

Odds are you have a lot of Windows computers in your organization. In Chapter 4, *Windows*, on page ?, you'll learn about configuration choices you can make to keep your Windows computers more secure.

Finally, in Chapter 5, *Phishing*, on page ?, you'll see what phishing is and what attackers typically try to achieve with phishing emails. You'll learn what your organization should cover in its phishing training and what defenses you can put in place to make your organizations more resistant to phishing attacks.

Online Resources

The book's website has the source code for this book.[1] You can also use the book's website to post errata in case you find any issues while reading the book.

Now let's dig in and start making your organization more secure.

1. https://pragprog.com/book/rzsecur/pragmatic-security