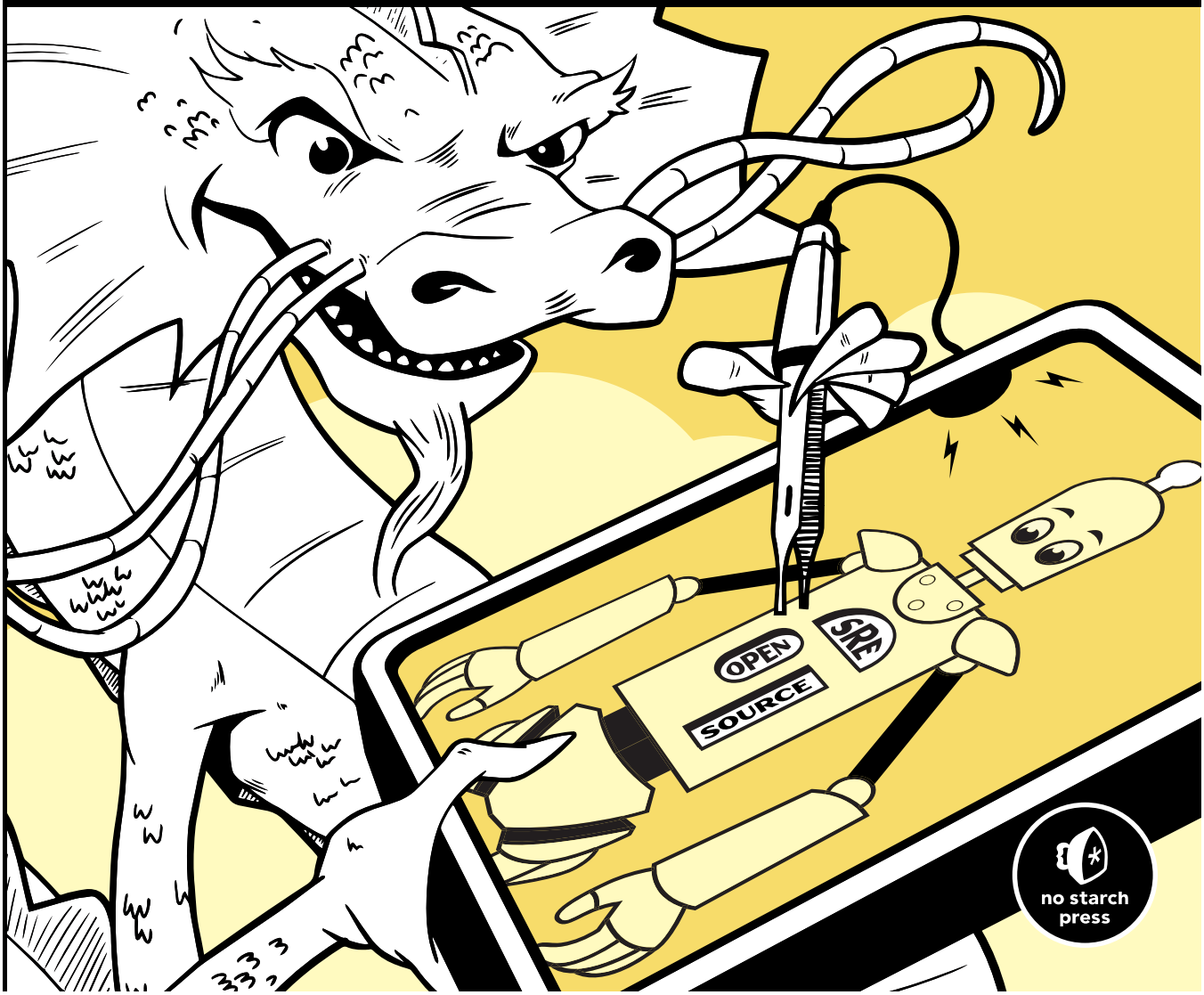
THE GHIDRA BOOK

THE *DEFINITIVE* GUIDE

CHRIS EAGLE AND KARA NANCE



no starch press

THE GHIDRA BOOK

The Definitive Guide

by Chris Eagle and Kara Nance

no starch
press

San Francisco

THE GHIDRA BOOK.

ISBN-13: 978-1-71850-102-7 (print)
ISBN-13: 978-1-71850-103-4 (ebook)

Publisher: William Pollock
Executive Editor: Barbara Yien
Production Editors: Laurel Chun and Katrina Taylor
Cover Illustration: Gina Redman
Interior Design: Octopod Studios
Project Editor: Dapinder Dosanjh
Developmental Editor: Athabasca Witschi
Technical Reviewer: Brian Hay
Copyeditor: Barton D. Reed
Compositor: Danielle Foster
Proofreader: Sharon Wilkey

For information on distribution, translations, or bulk sales, please contact No Starch Press, Inc. directly:
No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
phone: 1.415.863.9900; info@nostarch.com
www.nostarch.com

Library of Congress Control Number: 2020938508

INTRODUCTION

Our goal in writing this book is to provide a resource that introduces Ghidra to both current and future reverse engineers. In the hands of a skilled reverse engineer, Ghidra streamlines the analysis process and allows users to customize and extend its capabilities to suit their individual needs and improve their workflows. Ghidra is also very accessible to new reverse engineers, particularly with its included decompiler that can help them more clearly understand the relationships between high-level language and disassembly listings as they begin exploring the world of binary analysis.

Writing a book about Ghidra is a challenging undertaking. Ghidra is a complex open source reverse engineering tool suite that is continually evolving. Our words describe a moving target, as the Ghidra community continues to improve and extend its capabilities. As with many new open source projects, Ghidra has begun its public life with a rapid string of evolutionary releases. A primary goal while writing this book has been to ensure that as Ghidra evolves, the book's content continues to provide readers with a wide

and deep foundation of knowledge to understand and effectively utilize current and future Ghidra versions to address their reverse engineering challenges. As much as possible, we have tried to keep the book version-agnostic. Fortunately, new releases of Ghidra are well-documented, with detailed listings of changes that provide version-specific guidance should you encounter any differences between the book and your version of Ghidra.

About This Book

This book is the first comprehensive book about Ghidra. It is intended to be an all-encompassing resource for reverse engineering with Ghidra. It provides introductory content to bring new explorers to the reverse engineering world, advanced content to extend the worldview of experienced reverse engineers, and examples for rookie and veteran Ghidra developers alike to continue to extend Ghidra's extensive capabilities and become contributors to the Ghidra community.

Who Should Read This Book?

This book is intended for aspiring and experienced software reverse engineers. If you don't already have reverse engineering experience, that's okay, as the early chapters provide the background material necessary to introduce you to reverse engineering and enable you to explore and analyze binaries with Ghidra. Experienced reverse engineers who want to add Ghidra to their toolkits might choose to move quickly through the first two parts to gain a basic understanding of Ghidra and then jump to specific chapters of interest. Experienced Ghidra users and developers may choose to focus on the later chapters so that they can create new Ghidra extensions and can apply their experience and knowledge to contribute new content to the Ghidra project.

What's in This Book?

The book is divided into five parts. Part I introduces disassembly, reverse engineering, and the Ghidra project. Part II covers basic Ghidra usage. Part III demonstrates ways you can customize and automate Ghidra to make it work for you. Part IV takes a deeper dive into explaining specific types of Ghidra modules and supporting concepts. Part V demonstrates how Ghidra can be applied to some real-world situations a reverse engineer is likely to encounter.

Part I: Introduction

Chapter 1: Introduction to Disassembly
: This introductory chapter walks you through the theory and practice of disassembly and discusses some of the pros and cons associated with the two common disassembly algorithms.

Chapter 2: Reversing and Disassembly Tools
This chapter discusses the major categories of tools available for reverse engineering and disassembly.

Chapter 3: Meet Ghidra
Here you get to meet Ghidra and learn a little bit about its origin and how you can obtain and start using this free open source tool suite.

Part II: Basic Ghidra Usage

Chapter 4: Getting Started with Ghidra
Your journey with Ghidra begins in this chapter. You'll get your first glimpse of Ghidra in action as you create a project, analyze a file, and begin to understand the Ghidra graphical user interface (GUI).

Chapter 5: Ghidra Data Displays
Here you'll be introduced to the CodeBrowser, Ghidra's main tool for file analysis. You'll also explore the primary CodeBrowser display windows.

Chapter 6: Making Sense of a Ghidra Disassembly
This chapter explores the concepts that are fundamental to understanding and navigating Ghidra disassemblies.

Chapter 7: Disassembly Manipulation
In this chapter, you'll learn to supplement Ghidra's analysis and manipulate a Ghidra disassembly as part of your own analysis process.

Chapter 8: Data Types and Data Structures
In this chapter, you will learn how to manipulate and define simple and complex data structures found within compiled programs.

Chapter 9: Cross-References
This chapter provides a detailed look at cross-references, how they support graphing, and the critical role they play in understanding a program's behavior.

Chapter 10: Graphs
This chapter introduces you to Ghidra's graphing capabilities and the use of graphs as binary analysis tools.

Part III: Making Ghidra Work for You

Chapter 11: Collaborative SRE
This chapter presents a unique capability within Ghidra—using Ghidra as a collaborative tool. You will learn how to configure a Ghidra server and share projects with other analysts.

Chapter 12: Customizing Ghidra
Here you begin to see how you can customize Ghidra by configuring projects and tools to support your individual analysis workflows.

Chapter 13: Extending Ghidra's Worldview
This chapter teaches you how to generate and apply library signatures and other specialized content so that Ghidra can recognize new binary constructs.

Chapter 14: Basic Ghidra Scripting
In this chapter, you'll be introduced to the basic Ghidra scripting capabilities in Python and Java using Ghidra's inline editor.

Chapter 15: Eclipse and GhidraDev
This chapter takes your Ghidra scripting to a whole new level by integrating Eclipse into Ghidra and exploring the powerful scripting capabilities that this combination provides, including a worked example of building a new analyzer.

Chapter 16: Ghidra in Headless Mode
You'll be introduced to the use of Ghidra in headless mode, where no GUI is required. You will quickly understand the advantage of this mode for common large-scale repetitive tasks.

Part IV: A Deeper Dive

Chapter 17: Ghidra Loaders
Here you'll take a deep dive into how Ghidra imports and loads files. You will have the opportunity to build new loaders to handle previously unrecognized file types.

Chapter 18: Ghidra Processors
This chapter introduces you to Ghidra's SLEIGH language for defining processor architectures. You will explore the process for adding new processors and instructions to Ghidra.

Chapter 19: The Ghidra Decompiler
Here you'll be provided with a closer look at one of Ghidra's most popular features: the Ghidra Decompiler. You will see how it works behind the scenes and how it can contribute to your analysis process.

Chapter 20: Compiler Variations
This chapter helps you understand the variations you can expect to see in code compiled using different compilers and targeting different platforms.

Part V: Real-World Application

Chapter 21: Obfuscated Code Analysis
You'll learn how to use Ghidra to analyze obfuscated code in a static context so that the code doesn't need to be executed.

Chapter 22: Patching Binaries
This chapter teaches you some methods for using Ghidra to patch binaries during analysis, both within Ghidra itself and to create new patched versions of the original binaries.

Chapter 23: Binary Differencing and Version Tracking
This final chapter provides an overview of the Ghidra features that allow you to identify differences between two binaries as well as a brief introduction to Ghidra's advanced version tracking capabilities.

Appendix: Ghidra for IDA Users
If you are an experienced IDA user, this appendix will provide you with tips and tricks for mapping IDA terminology and usage to similar functionality in Ghidra.

NOTE *Visit the companion sites,* https://nostarch.com/GhidraBook/ *and* https://ghidrabook.com/*, to access the code listings contained in this book.*

11

COLLABORATIVE SRE

At this point, you should be comfortable navigating the Ghidra project environment and the many available tools and windows. You know how to create a project, import files, navigate, and manipulate the disassembly. You understand Ghidra data types, data structures, and cross-references. But do you understand scale? A 200MB binary is likely to generate a disassembly that is millions of lines long and consists of hundreds of thousands of functions. Even with the largest, portrait-oriented monitor you can find, you'll be able to view only a few hundred lines of that disassembly at any one time.

One way to take on such a monumental task is to assign a team of people to it, but that introduces an additional problem: how will you synchronize everyone's efforts so that people aren't walking all over one another with their changes? It's time to extend our discussion of using Ghidra to cover a collaborative team working together on a shared project. Ghidra's support for collaborative reverse engineering alone makes it unique among software analysis tools. In this chapter, we introduce Ghidra's collaboration

server, which is included with the standard Ghidra distribution. We discuss its installation, configuration, and use to help you get more eyes focused on your most challenging RE problems.

Teamwork

SRE is a complex process, and few individuals are experts in all of its intricacies. The ability to have analysts with different skill sets simultaneously analyzing a single binary can drastically reduce the amount of time needed to obtain the desired results. A rock star in navigating control flows through a complex program may dread having to analyze and document the associated data structures. An expert in malware analysis may be ill-suited for vulnerability discovery work, and anyone who is pressed for time is less likely to use that time inserting the inevitable plethora of comments that will certainly be useful down the road, but may in the short run keep them from analyzing additional code. Five colleagues may want to individually analyze the same binary but recognize that there are certain steps in the process that they will all need to do. An individual may need to pass off an assignment to a colleague for expert input or while on vacation. Sometimes, it is just helpful to have multiple sets of eyes looking at the same thing for sanity checks. Regardless of the motivation, the shared project capability within Ghidra supports collaborative SRE in many forms.

Ghidra Server Setup

Collaboration in Ghidra is facilitated by a shared Ghidra Server instance. If you are the system administrator responsible for setting up the Ghidra Server, you have a lot of choices to make, like whether to deploy it on a bare-metal server or in a virtual environment for ease of migration and repeatable installation. The deployment we use in this chapter to demonstrate Ghidra's collaborative features is suitable for development and experimentation only. If you are configuring a Ghidra Server for production use, you should carefully read the Ghidra Server documentation and determine an appropriate configuration for your environment and specific use case. (An entire book could be written to describe Ghidra Server setup and all the installation options and associated approaches, but that isn't this book.)

Although Ghidra Server can be configured on all platforms that support Ghidra, we will describe running a Ghidra Server instance in a Linux environment and assume some familiarity with the Linux command line and system administration. We will make a few minor modifications to the Ghidra Server configuration file (specified in *server/server.conf*) to facilitate the concepts that we want to demonstrate in this chapter so that we are not overly reliant on use of the Linux command line interface after we complete the initial installation, configuration, administration, and access control. Modifications include changing the default Ghidra repository directory to one of our own choosing, as recommended in the Ghidra Server documentation, and tuning user management and access control settings.