IRE

A Framework For Inductive Reverse Engineering

by

Connor Nelson

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved April 2019 by the
Graduate Supervisory Committee:

Adam Doupé, Chair
Yan Shoshitaishvili
Ruoyu Wang

ARIZONA STATE UNIVERSITY

May 2019

ABSTRACT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc.

Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat

magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque i tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus.

Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa. Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tin- cidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollic- itudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hen- drerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor.

DEDICATION

Here is a dummy dedication. The dedication can be vertically centered like this text is. See the LaTeX code for this dedication to see how to vertically center the text of your dedication.

ACKNOWLEDGMENTS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices biben- dum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

Chapter 1

INTRODUCTION

Reverse engineering is a methodology for precisely analyzing the internal workings and substructure of a process or system in order to better understand how it works. In practice, it is done in the absence of high-level specifications and can be thought of as working backwards through the standard engineering process—design towards implementation—and instead, implementation towards design. In theory, reverse engineering is relatively straightforward: simply observe how the internals are operating and how the subcomponents are connected. Of course, it is more nuanced than this; but even so, a complete working system that can be observed is, by its very nature, perfectly descriptive of what it does and how it works. This is an underlying requirement of standard reverse engineering. In hardware, a physical object is disassembled and examined. In software, its source code is read through, or in its absence, binary disassembled and machine code analyzed.

Consider, however, the task of reverse engineering without complete access to observing the system. This is the case in distributed systems, where some agent has only partial access to the overall system. Take for instance web applications, where a client makes a request to a server and is only made aware of its response. From the client's perspective, the server is merely a black box—an oracle—that takes some input and returns some output. What happens in between is left unknown to the client. In such cases, reverse engineering becomes inherently uncertain.

Further consider the problem of systems in which interactions take place between persons and computers; for instance, a human interacting with some computer pro-

gram in a repetitive way. This constitutes a distributed system, where part of the program takes place in the computer, but also part of it takes place in the person's intentions towards interacting with the computer. In such cases, the program occurring in the person's intentions—in the person's mind—is but a black box to the computer. It is in this way that reverse engineering may be applied not only towards analyzing a computer, but also a person. Reverse engineering may be useful here in order to profile or improve upon the user experience of the person.

Chapter 2

BACKGROUND

This sort of reverse engineering without access to internals has become a massively important skill, and in particular, critical to cybersecurity. Take for instance phone phreaking, where early hackers mapped out the phone network and how it worked simply by interacting with it using various tones and observing the results. In more recent times, penetration testing has become an important profession which often relies on reverse engineering in order to audit the security of companies from the perspective of an outside attacker.

In response to the demand for reverse engineering, recent efforts have been made to push towards Cyber Reasoning Systems which aid in this effort, and in some cases entirely automate it. The Defense Advanced Research Projects Agency (DARPA) led an initiative to develop fully autonomous systems capable of reverse engineering and exploiting challenge binaries in their Cyber Grand Challenge **shellphish2017cyber** This has led to significant advances in program analysis and various techniques surrounding state-of-the-art reverse engineering. Many of these techniques can be seen in open source frameworks for performing program analysis including *angr* and *Manticore* **stephens2016driller** These frameworks provide users with tools for precisely reasoning about a program by analyzing their internals.

Chapter 3

THEORIES AND THEORISTS

Chapter 4

CONVERSATIONS

Chapter 5

GRAMMARLESS

REFERENCES