國立交通大學

網路工程研究所

碩 士 論 文

軟 體 除 錯 與 符 號 執 行 整 合 互 動

Interacting Software Debugging with Symbolic Execution

研 究 生：陳威伯

指導教授：黃世昆　教授

中 華 民 國 106 年 5 月
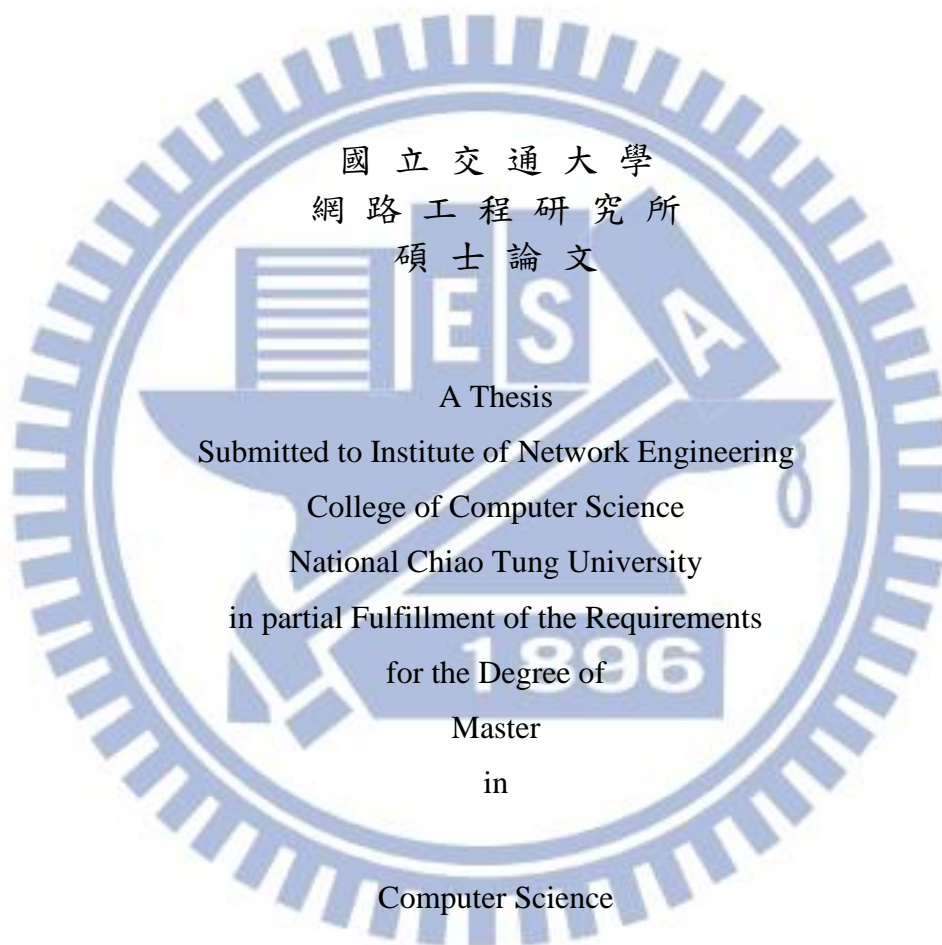
軟 體 除 錯 與 符 號 執 行 整 合 互 動
Interacting Software Debugging with Symbolic Execution

研 究 生：陳威伯　　　　Student：Wei-Bo Chen

指導教授：黃世昆　　　　Advisor：Shih-Kun Huang

國 立 交 通 大 學
網 路 工 程 研 究 所
碩 士 論 文

A Thesis

Submitted to Institute of Network Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

May 2017

Hsinchu, Taiwan, Republic of China

中 華 民 國 106 年 5 月

軟體除錯與符號執行整合互動

研究生：陳威伯　　　　　　　指導教授：黃世昆教授

國立交通大學網路工程研究所碩士班

摘要

這是摘要

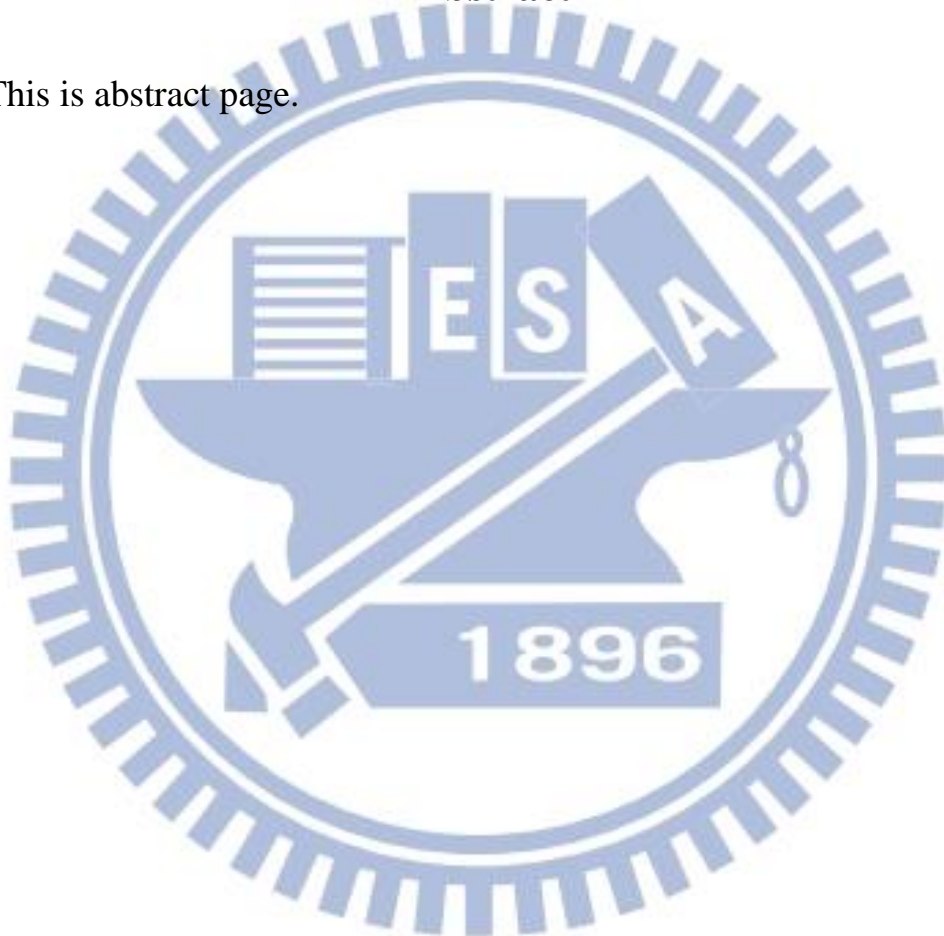# Interacting Software Debugging with Symbolic Execution

Student: Wei-Bo Chen

Advisor: Dr. Shih-Kun Huang

Institute of Network and Engineering
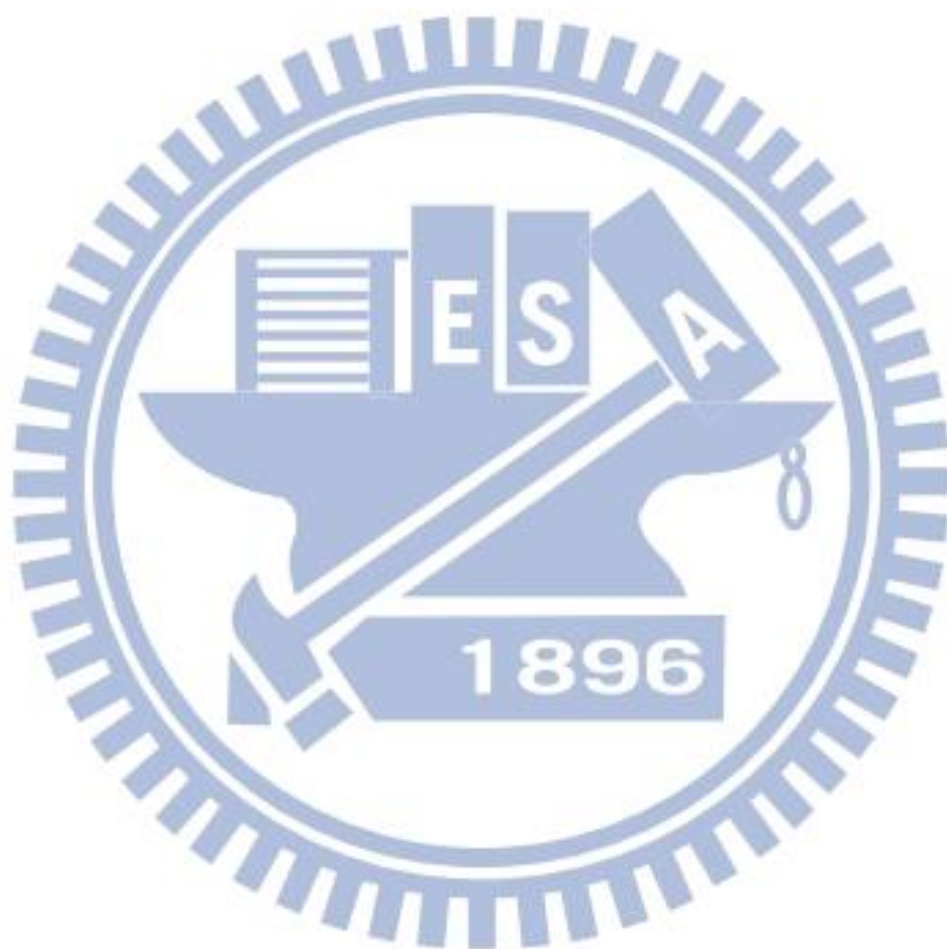
National Chiao Tung University

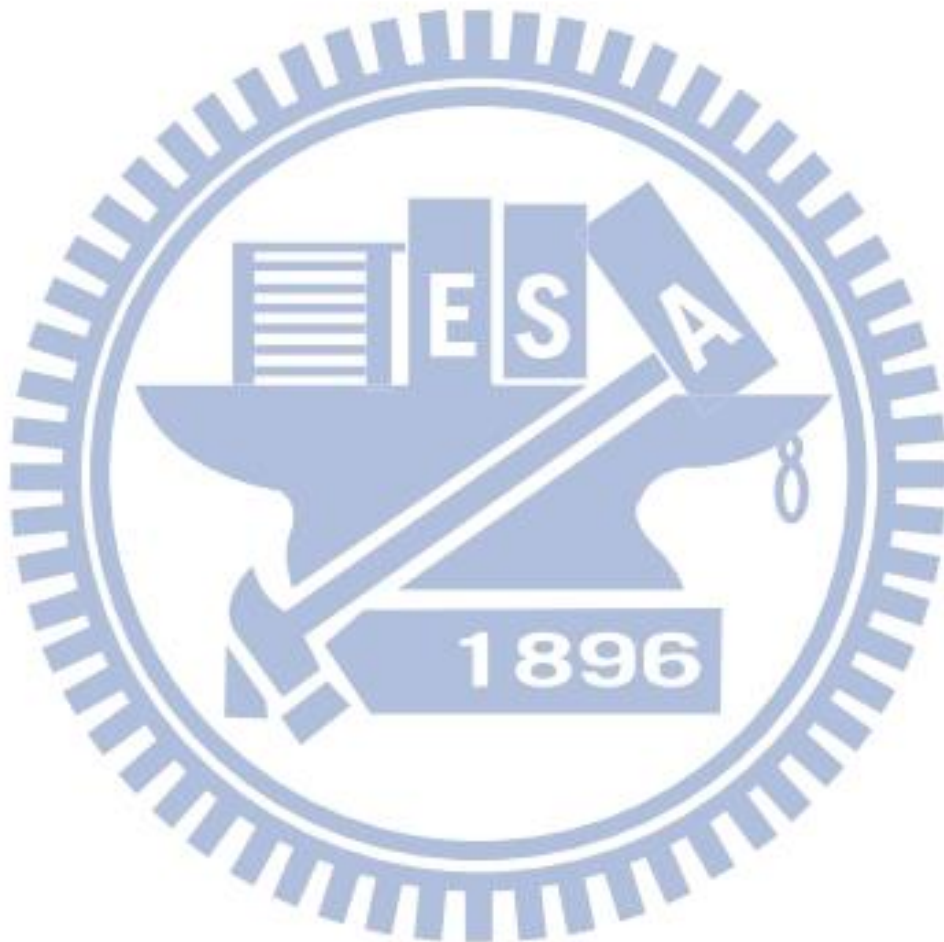## Abstract

This is abstract page.

致謝

List of Contents

List of Figures

List of Tables

1. Introduction

Introduction content

2. Background

Background content

2.1 Qira

Qira content

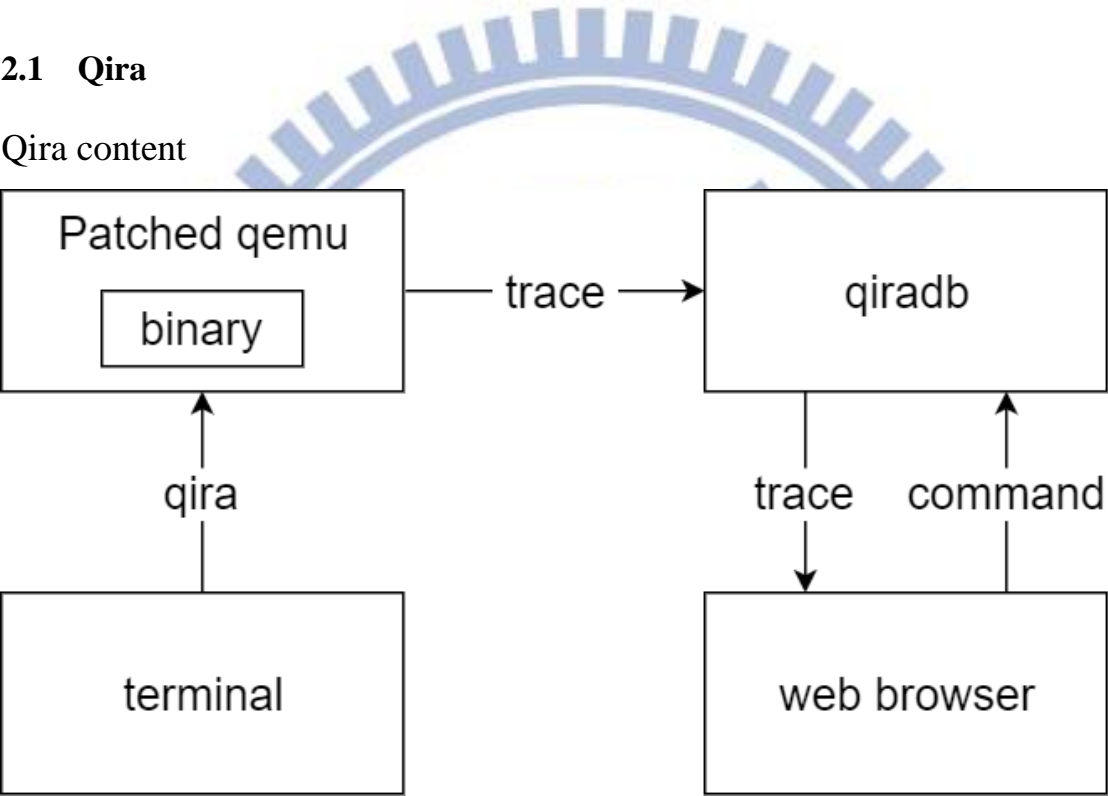

Figure 1: qira structure

2.2 Symbolic execution

Symbolic execution content

2.3 Ponce

Ponce content

3. Design

Design content

3.1 Overview

Overview content

3.2 Structure

Structure content

3.3 Internal

Internal content

3.4 Commands

Commands content

Table 1: Commands

Commands	Parameter	Emphasis
symbolize	argv	Automatically symbolize argv[0]
	memory [address] [size]	Symbolize memory from address to address+size
target	address	Set target address
triton	None	Run symbolic execution

4. Evaluation

Evaluation content

4.1 Crackme hash

Crackme hash content

4.2 Crackme xor

Crackme xor content

5. Related work
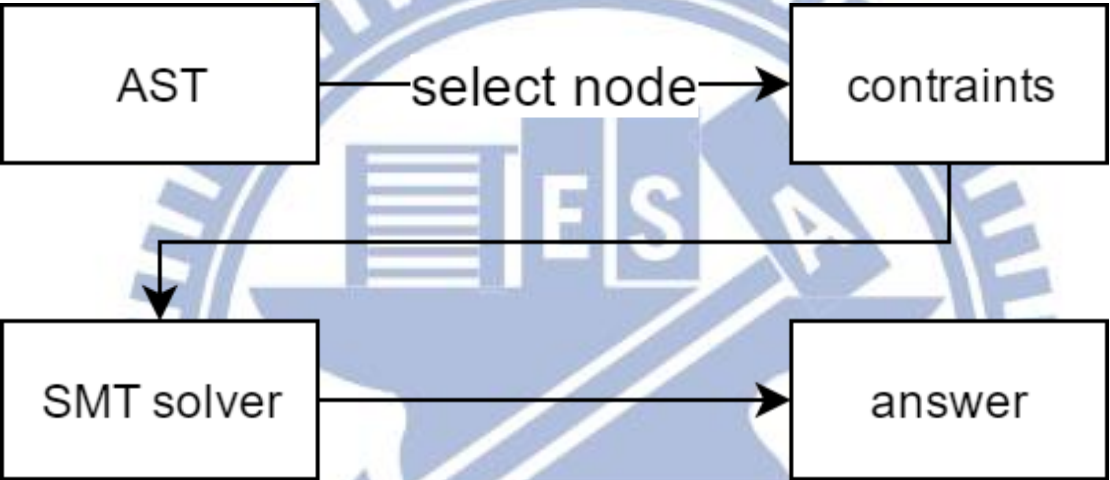
Related work content

5.1 Triton

Triton content

Figure 2: SMT solver

5.2 Ponce

Ponce content

5.3 Peda

Peda content

6. Conclusion

Conclusion content

7. Future work

Future work

8. References

Reference list