SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Automated Test Case Generation for Emulators Using Symbolic Execution

Alp Berkman

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Automated Test Case Generation for Emulators Using Symbolic Execution

Automatische Testgenerierung für Emulatoren mit Hilfe von Symbolic Execution

Author:	Alp Berkman
Supervisor:	Prof. Dr.-Ing. Pramod Bhatotia
Advisor:	Sebastian Reimers, M.Sc. & Theofilos Augoustis, M.Sc.
Submission Date:	14th March 2024

I confirm that this bachelor's thesis is my own work and I have documented all sources and material used.

Munich, 14th March 2024 Alp Berkman

Acknowledgments

Thank the chair for the opportunity Thank sebastian for supervising me Thank Theo for helping me when Seb is busy and the meetings Thank Nicola for always helping me and answering my questions

Major thanks Big thanks Minor thanks

I am deeply indebted to I would like to express my deepest appreciation to I would like to express my deepest gratitude to I'm extremely grateful to This endeavor would not have been possible without I could not have undertaken this journey without Words cannot express my gratitude to

Many thanks to Special thanks to I am also thankful to/for I am also grateful to/for Thanks should also go to I would like to extend my sincere thanks to

I'd like to acknowledge Lastly, I'd like to mention I'd like to recognize I had the pleasure of working with/collaborating with I would be remiss in not mentioning

Abstract

Contents

Acknowledgments **iv**

Abstract **v**

1 Introduction **1**

2 Background **2**
2.1 Qemu 2
2.2 Binary Translation 2
2.3 Dynamic Execution 2
2.4 Symbolic Execution 2
2.5 Concolic Execution 2
2.6 lldb 2
2.7 miasm 2

3 Overview **3**

4 Design **4**

5 Implementation **5**

6 Evaluation **6**

7 Related Work **7**

8 Summary and Concluison **8**

9 Future Work **9**

10 Qemu **10**
10.1 Bugs 10
10.2 Translation TCG 10

11 Reproducer **11**

12 Introduction **12**
12.1 Section 12
12.1.1 Subsection 12

Abbreviations **14**

List of Figures **15**

List of Tables **16**

Bibliography **17**

1 Introduction

2 Background

2.1 Qemu

2.2 Binary Translation

2.3 Dynamic Execution

2.4 Symbolic Execution

2.5 Concolic Execution

2.6 lldb

2.7 miasm

3 Overview

4 Design

5 Implementation

6 Evaluation

7 Related Work

8 Summary and Concluison

9 Future Work

10 Qemu

10.1 Bugs

10.2 Translation TCG

11 Reproducer

12 Introduction

12.1 Section

Citation test [Lam94].

Acronyms must be added in `main.tex` and are referenced using macros. The first occurrence is automatically replaced with the long version of the acronym, while all subsequent usages use the abbreviation.

E.g. `\ac{TUM}, \ac{TUM}` ⇒ Technical University of Munich (TUM), TUM

For more details, see the documentation of the `acronym` package[1].

12.1.1 Subsection

See Table 12.1, Figure 12.1, Figure 12.2, Figure 12.3.

Table 12.1: An example for a simple table.

A	B	C	D
1	2	1	2
2	3	2	3

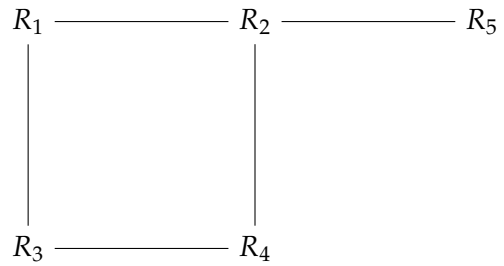

Figure 12.1: An example for a simple drawing.

[1] `https://ctan.org/pkg/acronym`

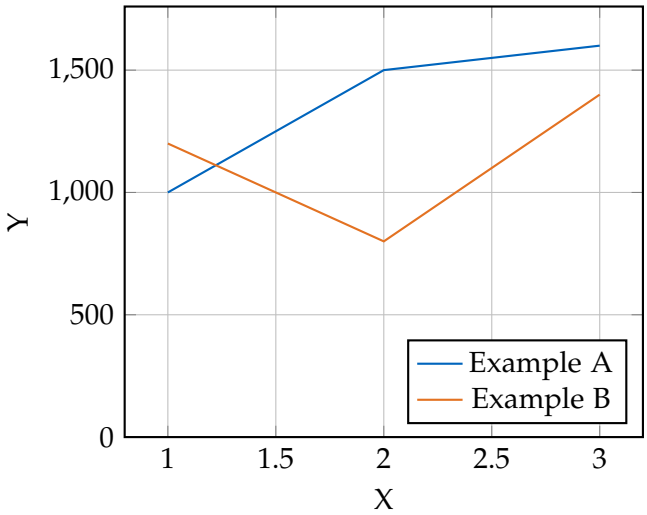

Figure 12.2: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 12.3: An example for a source code listing.

Abbreviations

TUM Technical University of Munich

List of Figures

12.1 Example drawing 12
12.2 Example plot 13
12.3 Example listing 13

List of Tables

12.1 Example table 12

Bibliography

[Lam94] L. Lamport. *LaTeX : A Documentation Preparation System User's Guide and Reference Manual*. Addison-Wesley Professional, 1994.