Table of Contents

Abstract **ii**

Dedication **iii**

Acknowledgments **iv**

Table of Contents **v**

List of Tables **vii**

List of Figures **viii**

Abbreviations **ix**

1 Introduction **1**

2 Background **2**

2.1 Introduction 2

2.2 Literature Review 2

2.3 AFL 7

2.3.1 Stages of fuzzing with AFL 8

2.4 LLVM 13

2.4.1 Instrumentation and coverage measurements 14

2.5 Concluding remarks 16

3 Proposed Fuzzer **17**

3.1 Introduction 17

3.2 Motivating example 18

3.3 Instrumentation 19

3.3.1 Features 19

3.3.1.1 Memory consumption 19

3.3.1.2 Instruction counters 20

3.4 Fuzzing the target 22

3.5 Concluding remarks 22

4 Simulation 23

4.1 Introduction 23

4.2 Target program and instrumentation 24

4.3 Program inputs and setups 24

4.4 Generating fuzzed data 24

4.5 Program execution and monitoring 24

4.6 Report vulnerabilities 24

5 Results and Evaluation 25

6 Conclusions and Future Work 26

Bibliography 27

A Handling stack operations in Memlock 31

Glossary 34

Vita