boa

Buffer Overrun Analyzer

Edo Cohen	Tzafrir Rehan	Gai Shaked
039374814	039811880	036567055
sedoc@t2	tzafrir@cs	gai@tx

February 23, 2011

Chapter 1

Introduction

1.1 Goal

Given a C program that performs buffer manipulations, statically (at compile time) identify whether the program may perform array access out of the array bounds.

1.2 Previous work

Chapter 2

boa

2.1 Overview

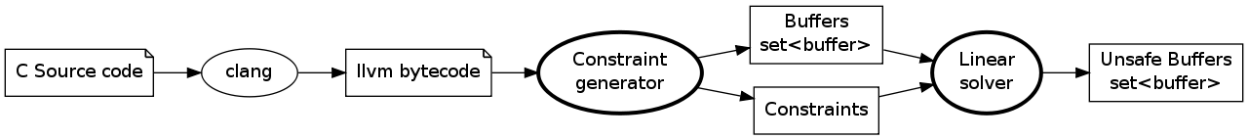

Figure 2.1: Main components and stages

2.2 Constraint Generator

2.2.1 Integers

2.2.2 Direct array access

```
1         char buf[10];
2         buf[10] = 'a';
```

2.2.3 String manipulation functions

```
1 #include "string.h"
2
3 int main() {
4   char *str1 = "longer than ten", *str2 = "short";
5   char buf1[10], buf2[10];
6   strcpy(buf1, str1);
7   strcpy(buf2, str2);
8 }
```

2.2.4 Buffer aliasing

2.3 Linear Solver

2.3.1 GLPK

2.3.2 Elastic filter

2.3.3 Blame system

2.4 Implementation

Chapter 3

-To be named-

3.1 Test system

3.2 Version control

3.2.1 Code reviews

Chapter 4

Results

4.1 fingerd

4.2 flex

Bibliography

[1] Buffer Overrun Detection using Linear Programming and Static Analysis