**Дудина Ирина Александровна Поиск ошибок переполнения буфера в исходном коде программ с помощью символьного выполнения**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Дудина Ирина Александровна

Введение

Глава 1. Ошибка переполнения буфера и подходы к её обнаружению

1.1 Обзор существующих подходов к поиску переполнения буфера

1.1.1 Динамический анализ

1.1.2 Статический анализ

1.1.3 Межпроцедурный анализ и контекстная чувствительность

1.2 Требования к детектору переполнения буфера

1.2.1 Тестовые наборы для оценки инструментов поиска переполнения буфера

1.2.2 Исследование уязвимостей, связанных с переполнением буфера

Глава 2. Определение ошибки доступа к буферу

2.1 Внутрипроцедурные ошибки

2.2 Межпроцедурные ошибки

Глава 3. Поиск ошибок в рамках одной функции

3.1 Модельный язык

3.2 Общий алгоритм анализа функции

3.2.1 Абстрактное состояние анализа

3.2.2 Построение достаточных условий ошибки

3.2.3 Структура множества Summary и построение условий U, L

3.3 Передаточные функции

3.3.1 Инструкция условного перехода

3.3.2 Инструкции выделения памяти

3.3.3 Инструкции присваивания и записи значения указателя

3.3.4 Инструкции присваивания, чтения и записи значения переменной

3.3.5 Инструкции арифметики битовых векторов

3.3.6 Инструкции обращения к массивам

Стр.

3.3.7 Слияние состояний

3.4 Анализ циклов

3.5 Корректность анализа

3.6 Пример обнаружения ошибки

Глава 4. Поиск межпроцедурных ошибок

4.1 Метод резюме

4.2 Ошибки с межпроцедурным вычислением индекса

4.3 Переполнение буфера, переданного как параметр функции

4.3.1 Переполнение при использовании библиотечных функций

Глава 5. Расширения базового алгоритма

5.1 Переполнение при работе со строками языка C

5.1.1 Расширение абстрактного состояния для работы со строками

5.1.2 Расширение отображения V для поиска ошибок переполнения при работе со строками

5.1.3 Расширение передаточных функций анализа для

поддержки строк

5.1.4 Поддержка анализа строк с широкими символами

5.2 Обнаружение переполнения данными, полученными из недоверенного источника

5.3 Поиск переполнения буфера в циклах

Глава 6. Анализ переполнения буфера произвольного размера

6.1 Использование отображения V для размера буфера

6.2 Перебор значений условий переходов

Глава 7. Реализация и результаты

7.1 Реализация методов поиска переполнения в анализаторе Svace

7.1.1 Анализатор Svace

7.1.2 Особенности реализации поиска переполнения буфера

7.2 Оценка качества анализатора с помощью тестовых пакетов и сравнение с Infer

7.3 Результаты тестирования на проектах Android и Tizen

Стр.

Заключение

Благодарности

Список литературы

Приложение А. Результаты на пакете Juliet Test Suite