УТВЕРЖДАЮ

проректор РТУ МИРЭА

Н.И. Прокопов

_____2023 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА - Российский технологический университет»

на диссертацию Чан Ти Тхиена по теме «Разработка нового метода автоматизированного тестирования программных библиотек», представленную к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Актуальность темы диссертационной работы обусловлена тем, что она позволяет в значительной мере решить часто возникающие при тестировании программных библиотек проблемы, отнимающие большое количество времени у разработчика и тестировщика, которое необходимо для изучения исходного кода, разработки фаззинг-оберток для функций библиотеки и для анализа результатов фаззинга.

Научная новизна. В диссертационной работе:

1. Предложен метод генерации фаззинг-оберток для функций библиотеки, который позволяет генерировать нацеленные тесты в условиях отсутствия информации о контексте использования библиотеки.
2. Предложен метод генерации фаззинг-оберток для функций библиотеки с учетом контекста использования библиотеки в пользовательской программе, который позволяет нацелить генератор только на используемые интерфейсы библиотеки.

Структура работы:

Диссертация состоит из введения, 5 глав, заключения и двух приложений. Полный объём диссертации составляет 114 страниц, включая 24 рисунка, 31 листинг и 3 таблицы. Список литературы содержит 74 наименования.

Во введении описывается актуальность проблемы, формулируются цель и задачи диссертационной работы, указана научная новизна результатов исследования, раскрыта их теоретическая значимость, и приводятся основные положения, выносимые на защиту.

В первой главе проводится обзор предметной области и работ по теме диссертации, а также рассматриваются существующие инструменты генерации фаззинг-оберток.

Вторая глава посвящена исследованию вопроса проведения анализа исходного кода библиотек для выделения программных сущностей и их взаимосвязей, необходимых для конструирования вызовов функций, подлежащих фаззинг-тестированию и для подготовки данных для генераторов фаззинг-оберток. Ключевой фокус рассмотрения – это анализ абстрактного синтаксического дерева и инструменты, которые упрощают решение этой задачи.

В третьей главе описывается разработанный метод генерации фаззинг-оберток для функций библиотеки в условиях отсутствия контекста использования. Рассматриваются процесс конструирования вызовов для функций библиотек и способы конструирования, подходящие как для простых, так и для сложных функций. В главе также описываются способы инициализации переменных типов для принятия мутационных данных из фаззера.

В четвертой главе описывается разработанный метод генерации фаззинг-оберток для функций библиотеки с учетом контекста использования. Автор описывает способ определения контекста использования тестируемой библиотеки путем анализа графа потока управления и графа потока данных. Контекст использования состоит из инициализируемых переменных и слайсинговых инструкций. Предложенный автором метод позволяет повысить эффективность генерации фаззинг-оберток за счет учета информации об использовании библиотеки в заданных пользовательских программах.

В пятой главе описывается архитектура и возможности реализованного программного средства Futag. Данное программное средство состоит из набора разработанных инструментов анализа исходного кода библиотеки и Python-модулей для генерации, компиляции и сбора результатов выполнения фаззинг-оберток. Показано, что представленные возможности сокращают трудоемкость написания фаззинг-оберток для функций тестируемых библиотек.

В заключении диссертации приводятся основные результаты и выводы проведенной работы.

Основные результаты диссертационной работы:

1. Предложен метод генерации фаззинг-оберток для функций библиотеки в условиях отсутствия контекста использования.
2. Предложен метод генерации фаззинг-оберток для функций библиотеки с учетом контекста использования.
3. Разработана программа Futag для реализации предложенных методов.

Достоверность результатов исследования:

Теоретическую и методологическую основу проведенных разработок и исследований составили труды отечественных и зарубежных авторов в области теории компиляторов, а также решения, созданные и опубликованные в российских и зарубежных патентах и свидетельствах на изобретения РФ. Положения и выводы, сформулированные в диссертации, получили квалифицированную апробацию на международных и российских научных конференциях и семинарах. Достоверность также подтверждается публикациями результатов исследования в рецензируемых научных изданиях.

Замечания:

1. В работе не предлагается способа генерации фаззинг-оберток для шаблонных функций языка C++.
2. Не приводятся оценки сложности предложенных алгоритмов генерации фаззинг-оберток, которые представляют интерес, особенно в случае учета контекста использования.
3. Не рассматриваются случаи противоречивых контекстов использования библиотек пользовательскими программами – например, случаи, когда сложные структуры данных инициализируются разными способами в разных контекстах.

Заключение

Отмеченные недостатки не снижают положительной оценки диссертационной работы. Диссертация является законченным исследованием, выполненным автором самостоятельно, на высоком научном и методическом уровне. Результаты диссертационного исследования представлены статьями автора в рецензируемых научных журналах, а также обсуждались на всероссийских и международных конференциях. Автореферат диссертации правильно и полно отражает содержание работы и оформлен надлежащим образом.

Диссертация Чан Ти Тхиена является научно-квалификационной работой, в которой содержится решение важной научной задачи по автоматизации тестирования программных библиотек при помощи генерации фаззинг-оберток в условиях наличия и отсутствия данных о контексте использования функций библиотек, имеющей значение для развития технической отрасли знаний. Диссертационная работа Чан Ти Тхиен соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по научной специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а ее автор Чан Ти Тхиен заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Диссертационная работа и отзыв рассмотрены и утверждены на заседании кафедры КБ-14 «Цифровые технологии обработки данных» Федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет» (протокол №02/23-24 от 12 сентября 2023 года).

Заведующий кафедрой КБ-14
«Цифровые технологии обработки данных»
РТУ МИРЭА
кандидат технических наук, доцент И.А. Иванова

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет»
Адрес: 119454, ЦФО, г. Москва, Проспект Вернадского, д. 78
Телефон: +7 (499) 600-80-80
E-mail: rector@mirea.ru
Веб-сайт: https://www.mirea.ru/