Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук
Маркина Дмитрия Олеговича
на диссертационную работу Чан Ти Тхиена
по теме "Разработка нового метода автоматизированного тестирования программных библиотек ",
представленную к защите на соискание ученой степени кандидата технических наук по специальности 2.3.5 – "Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей"

Актуальность темы исследования

Большинство современных программных продуктов содержит подключаемые программные библиотеки, в том числе сторонние. Их количество может достигать нескольких сотен. При выполнении требований к реализации процедур жизненного цикла разработки безопасного программного обеспечения программные библиотеки, как и программы, в которых они используются, подлежат анализу на предмет наличия дефектов, потенциальных уязвимостей. Особенностью исследования программных библиотек является требование по наличию среды (программы), которая управляет ее запуском. Эта особенность не позволяют применять ряд методов динамического анализа библиотек и, в частности, фаззинг-тестирование, в том виде, в котором они используются в отношении программного обеспечения. Для исследования экспертам требуется разрабатывать так называемые программы-обертки (фаззинг-обертки), позволяющие применять фаззинг-тестирование к программным библиотекам. Имеющиеся в настоящее время средства автоматизации генерации фаззинг-оберток обладают принципиальными недостатками, не позволяющими эффективно генерировать программы-обертки для современного программного обеспечения. В связи с этим задача автоматизации генерации адекватных фаззинг-оберток является актуальный и требует разработки новых методов и подходов, учитывающих особенности современных программных библиотек.

В рассматриваемой работе целью является автоматизация тестирования программных библиотек при помощи генерации фаззинг-оберток как в условиях наличия, так и в условиях отсутствия данных о контексте использования функций библиотек.

Основные результаты

Результаты диссертационного исследования включают три положения, каждое из которых направлено на совершенствование технологии фаззинг-тестирования программных библиотек за счет автоматизации генерации фаззинг-оберток функций библиотек как в условиях наличия,

так и в условиях отсутствия данных о контексте использования функций исследуемых программных библиотек.

Диссертационная работа состоит из введения, пяти глав, заключения и списка литературы.

Во введении обосновывается актуальность, определяется цель работы, формулируются основные научные результаты.

Первая глава содержит анализ программных библиотек как объектов исследования и известных инструментальных средств генерации фаззинг-оберток для них, их достоинств и недостатков.

Во второй главе представлено описание результатов анализа особенностей инструментов статического анализа, позволяющих выделять сведения о программных сущностях, их взаимосвязях, необходимых для конструирования вызовов, используемых при фаззинг-тестировании программных библиотек, и подготовки данных для средства генерации фаззинг-оберток.

Третья глава посвящена описанию разработанного автором метода генерации фаззинг-оберток функций библиотек в условиях отсутствия информации о контексте использования.

В четвертой главе описан разработанный автором метод генерации фаззинг-оберток для функций библиотеки с учетом контекста использования в программном обеспечении.

Пятая глава содержит описание программной реализации предложенных методов в программе Futag – генераторе фаззинг-оберток.

Заключение работы содержит краткое описание основных полученных результатов исследования.

Первое положение, выносимое на защиту, состоит в разработке метода генерации фаззинг-оберток функций библиотек в условиях отсутствия контекста использования.

Второе положение, выносимое на защиту, состоит в разработке метода генерации фаззинг-оберток функций библиотек с учетом контекста использования.

Третье положение, выносимое на защиту, заключается в разработке программного средства Futag, реализующего разработанные методы генерации фаззинг-оберток.

Личное участие соискателя ученой степени в получении результатов, изложенных в диссертации, полнота изложения материалов диссертации в работах, опубликованных соискателем

Соискателем по теме работы опубликовано 2 научных статьи в журналах, рекомендованных ВАК, индексируемых в Web of Science и Scopus. Зарегистрирована 1 программа для ЭВМ с единоличным авторством. Статьи подготовлены и опубликованы в соавторстве с научным руководителем и другими авторами. Результаты апробированы на шести открытых конференциях всероссийского и международного уровня. Тезисы

доклада на международной конференции "Engineering & Telecommunication En&T 2022" подготовлены автором единолично. В диссертационной работе описан вклад автора в каждой из публикации. В совокупности представленные результаты свидетельствуют о подготовке диссертации автором единолично и необходимом личном участии соискателя в получении результатов.

Основные результаты диссертационной работы и положений, выносимых на защиту, достаточно полно изложены в работах, опубликованных соискателем. Количество публикаций соискателя по основным результатам, полученным в работе, соответствует требованиям, предъявляемым для диссертаций на соискание ученой степени кандидата наук (пункт 13 Положения "О порядке присуждения ученых степеней", утвержденного постановлением Правительства Российской Федерации от 24.09.2013 года № 842).

Степень обоснованности научных положений, достоверность результатов, их новизна и практическая значимость

Содержание исследования изложено на достаточно высоком научном уровне с применением оригинального подхода к решению научной задачи, обоснованием эффективности предложенных решений, выводов и рекомендации. Представлены результаты достаточно глубокого анализа известных достижений в области решаемой задачи с указанием их основных достоинств и недостатков. Апробированный математический аппарат: теория алгоритмов, методы статического и динамического анализа программ, теория компиляторов применены соискателем корректно.

Сравнение полученных результатов по каждому положению, выносимому на защиту, с существующими аналогами выполнено экспертным методом в виду специфики объекта исследования, а также отсутствия доступа к западным инструментам-аналогам. Положительный эффект от их применения показан в форме повышения оперативности подготовки фаззинг-оберток функций библиотек по сравнению с ручным методом их разработки, а также за счет качественного сравнения получаемых результатов при применении известных аналогов и разработанного средства. С учетом изложенных особенностей полученные результаты можно считать достаточно *обоснованными* и *достоверными*.

Новизна первого положения, выносимого на защиту, состоит в применении нового подхода по генерации фаззинг-оберток функций библиотек в условиях отсутствия информации о контексте использования, заключающегося в использовании средств статического анализа для извлечения данных, необходимых для определения контекста вызова функции, с применением в дальнейшем полученной базы знаний для генерации фаззинг-обертки.

Новизна второго положения, выносимого на защиту, заключается в применении нового подхода по генерации фаззинг-оберток функций

библиотек с учетом контекста использования, заключающегося в последовательном применении методов анализа потока управления и потока данных в целях получения сведений о контексте использования, применении средств статического анализа, описанных в первом положении, с последующей генерацией на основе полученной базы знаний фаззинг-обертки.

Новизна третьего положения, выносимого на защиту, состоит в разработке программной реализации разработанных методов генерации фаззинг-оберток, а также исследовании эффективности реализованных методов.

Теоретическая значимость работы состоит в разработке новых методов генерации фаззинг-оберток функций программных библиотек, позволяющих автоматизировать процесс подготовки программных библиотек к фаззинг-тестированию.

Практическая значимость полученных результатов подтверждается наличием зарегистрированной программы для ЭВМ, разработанной соискателем единолично, результативность которой подтверждается представленными численными результатами в материалах диссертации и согласуется с теорией.

Научная специальность, которой соответствует диссертация

Основные результаты диссертационных исследований соответствуют паспорту научной специальности 2.3.5 – "Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей", а именно направлению исследований по пункту 1 – модели, методы и алгоритмы проектирования, анализа, трансформации, верификации и тестирования программ и программных сетей.

Замечания

1. В работе не представлено достаточного обоснования выбора средства статического анализа clang static analyzer в качестве основного источника сведений для базы знаний, используемой для генерации фаззинг-оберток в предложенных автором методов.

2. Отсутствует определение области применения предложенных методов генерации фаззинг-оберток. Из текста диссертации и автореферата непонятно каким требованиям должны отвечать исследуемые программные библиотеки, в каких средах функционирования (операционных системах) они функционируют, на каких аппаратных платформах и процессорных архитектурах запускаются.

3. Анализ полезного эффекта от применения программной реализации методов (средства Futag), разработанной соискателем, выполнен в ограниченном объеме. Сравнительный анализ полученных результатов генерации фаззинг-оберток функций библиотек в количественных показателях выполнен только для показателей оперативности. При этом

сравнение выполнено с результатами ручной генерации экспертом, а не результатами применения известных аналогов. Анализ результативности применения предложенных методов (корректности генерируемых фаззинг-оберток) по сравнению с известными аналогами выполнен качественном уровне экспертным методом. При этом отмечается, что для некоторых аналогов разработанный соискателем инструмент генерирует эквивалентные фаззинг-обертки.

Однако указанные недостатки не являются принципиальными и не снижают теоретической и практической значимости полученных результатов. Результаты в достаточной степени оригинальны, обладают научной новизной и практической значимостью, обоснованы, достоверны и демонстрируют вклад автора в области исследований методов и алгоритмов анализа, верификации и тестирования программ и программных систем.

Заключение о соответствие критериям

Содержание автореферата отражает суть диссертационной работы и позволяет достаточно ясно оценить основные полученные результаты и степень их обоснованности и достоверности.

Представленная диссертация соответствует статусу научно-квалификационной работы, в которой содержится решение научной задачи, имеющей значение для развития соответствующей отрасли знаний.

Диссертация написана автором самостоятельно, обладает внутренним единством, содержит новые научные результаты и положения, что подтверждает личный вклад соискателя в науку.

Работа имеет прикладной характер, основные результаты реализованы в виде программы для ЭВМ. Присутствуют сведения об их эксплуатации в испытательной лаборатории НТЦ "Фобос-НТ".

Диссертация отвечает критериям и требованиям Положения "О порядке присуждения ученых степеней", утвержденного постановлением Правительства Российской Федерации от 24.09.2013 года № 842 в редакции от 18.03.2023 года, предъявляемым к кандидатским диссертациям, а ее автор Чан Ти Тхиен, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.5 – "Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей".

Официальный оппонент
сотрудник ФГКВОУ ВО "Академия Федеральной службы охраны Российской Федерации"
кандидат технических наук Д. О. Маркин
"29" сентября 2023. г

Подпись Маркина Дмитрия Олеговича ЗАВЕРЯЮ
Начальник кадрового аппарата А.Б. Семибратов