Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук
Маркина Дмитрия Олеговича
на диссертационную работу Куца Даниила Олеговича
по теме "Метод моделирования косвенной адресации в рамках динамической символьной интерпретации",
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

Развитие современного программного обеспечения предъявляет повышенные требования к обеспечению его безопасности и применению эффективных методов его тестирования и исследования. Одним из наиболее эффективных методов тестирования является фаззинг. Однако из-за растущего уровня сложности современных программ фаззинг-тестирование не всегда достаточно эффективно, поскольку существующие подходы к его реализации не позволяют учесть все особенности исследуемых программных реализаций. Соответственно актуальным направлением исследований является развитие и разработка новых методов, повышающих эффективность фаззинга. К такому направлению относится тема рассматриваемой диссертационной работы, посвященной вопросам моделирования косвенной адресации в процессе символьной интерпретации. Решение задачи корректного моделирования косвенной адресации позволит с одной стороны учесть больше особенностей современных программ, с другой – при применении совместно с фаззингом повысит эффективность тестирования программного обеспечения.

Заявленная цель рассматриваемой работы состоит в разработке метода моделирования косвенной адресации в рамках динамической символьной интерпретации. Однако фактически достигаемый эффект от полученных в работе результатов состоит в увеличении показателя покрытия кода при фаззинг-тестировании и, соответственно, наличии возможности исследования большего количество кода программы на предмет наличия дефектов и/или уязвимостей.

Основные результаты

Результаты диссертационного исследования включают три положения, каждое из которых направлено на совершенствование процедур символьной интерпретации программного обеспечения, содержащего косвенную адресацию.

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

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

Первая глава посвящена глубокому анализу возможностей современных средств, обеспечивающих символьную интерпретацию, в контексте решения задачи обнаружения и моделирования косвенных переходов, их достоинств и недостатков.

Во второй главе представлено описание разработанного метода поиска и моделирования косвенных переходов с оценкой результатов его применения в составе средства анализа Sydr.

В третьей главе представлено описание разработанного автором метода моделирования чтений памяти по символьному адресу и экспериментальная оценка эффектов от его применения.

В четвертой главе описана программная реализация разработанных методов в составе инструмента динамической символьной интерпретации Sydr.

Заключение работы содержит краткое описание основных полученных результатов исследования.

Первое положение, выносимое на защиту, состоит в разработке метода поиска и моделирования косвенных переходов.

Второе положение, выносимое на защиту, состоит в разработке метода моделирования чтений памяти по символьно вычисляемому адресу, позволяющего учитывать косвенную адресацию при реализации символьной интерпретации программы.

Третье положение, выносимое на защиту, заключается в разработке программного инструмента, реализующего метод поиска и моделирования косвенных переходов и чтений по символьно вычисляемому адресу.

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

Соискателем по теме работы опубликовано 4 научных статьи в журналах, рекомендованных ВАК, индексируемых в Web of Science и Scopus. Зарегистрировано 4 программы для ЭВМ. Одна статья подготовлена и опубликована автором единолично, остальные – в соавторстве с научным руководителем и другими авторами. Результаты апробировались на достаточном количестве открытых конференций всероссийского и международного уровня. Представленные результаты свидетельствуют о подготовке диссертации автором единолично и необходимым 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 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: математическая логика, теории множеств и алгоритмов, а также методы динамического анализа программ, символьной интерпретации, гибридного фаззинга применены соискателем корректно. Полученные результаты по каждому положению, выносимому на защиту, сравнены с существующими аналогами, показан положительный эффект от их применения. Указанные обстоятельства свидетельствуют о надлежащей *обоснованности* и *достоверности* полученных результатов.

Новизна первого положения, выносимого на защиту, состоит в разработке нового подхода по обнаружению косвенных переходов в бинарном коде, основанного на определении основного алгоритма работы табличного перехода, а также в применении нового подхода по моделированию косвенных переходов, основанного на построении символьных ограничений, позволяющих обнаруживать входные данные для исполнения программы по альтернативным направлениям этих переходов.

Новизна второго положения, выносимого на защиту, заключается в разработке нового подхода по моделированию чтений по символьно вычисляемому адресу, заключающегося в последовательном применении двух этапов: определения примерной области памяти, из которой производится чтение, и построении соответствующего предиката пути.

Новизна третьего положения, выносимого на защиту, состоит в разработке программной реализации разработанных методов моделирования косвенных переходов и операций чтения по символьно вычисляемому адресу, а также исследовании эффективности реализованных методов.

Теоретическая значимость работы состоит в разработке новых методов моделирования косвенных переходов и операций чтения по символьно вычисляемому адресу, позволяющих при совместном

применении с методом фаззинга повысить показатель покрытия кода с приемлемым снижением производительности.

Практическая значимость полученных результатов подтверждается наличием 4 зарегистрированных программ для ЭВМ, соавтором которых является соискатель, реализующих предложенные методы, результативность которых 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 направлениям исследований по пунктам:

1 – модели, методы и алгоритмы проектирования, анализа, трансформации, верификации и тестирования программ и программных сетей;

5 – программные системы символьных вычислений.

Замечания

1. При поиске косвенных переходов в предложенном авторе методе рассматриваются только те базовые блоки, которые заканчиваются инструкциями call и jmp, а в качестве цели перехода выступает либо регистр, либо операнд доступа к памяти. Такой подход ограничивает область применения разработанного метода только в отношении программных реализаций для аппаратных платформ на базе процессоров с архитектурой x86_64 либо ее эмуляции. Соответственно, применение разработанных методов для иных процессорных архитектур (RISC-V, PowerPC, ELBRUS) невозможно.

2. Метод моделирования чтений из памяти по символьному адресу зависим от частных параметров (количества элементов памяти для моделирования символьного доступа), от которых с одной стороны зависит точность моделирования, а с другой – производительность его реализации. Соответственно, определение оптимальных параметров выполняется либо экспертным путем, либо на основе рекомендованных значений, что в отдельных случаях может снизить эффективность разработанного метода.

Однако указанные недостатки не являются принципиальными и не снижают теоретической и практической значимости полученных результатов. Результаты в достаточной степени оригинальны, обладают научной новизной и практически 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 четырех программ для ЭВМ. Присутствуют сведения об их эксплуатации в программных системах ИСП РАН.

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 Куц Даниил Олегович, 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
"28" сентября 2023. г

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