ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук
Маркина Дмитрия Олеговича
на диссертационную работу Вишнякова Алексея Вадимовича
по теме "Поиск ошибок в бинарном коде методами динамической символьной интерпретации",
представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 2.3.5 – "Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей"

Актуальность темы исследования

Современный уровень развития экономики требует автоматизации многочисленных процессов, в том числе с использованием информационных систем, обрабатывающих информацию, требующую защиты. В этих условиях необходимо выполнять требования к процедурам разработки безопасного программного обеспечения, заключающихся в систематическом поиске и выявлении ошибок, дефектов программного кода, уязвимостей, эксплуатация которых может нанести ущерб.

Одними из эффективных методов поиска ошибок в программном обеспечении являются методы фаззинга, позволяющие достаточно быстро находить ошибки разного типа. Однако в отношении современных программ в виду их растущей сложности применение метода часто встречается с ограничениями, снижающими его эффективность. Преодоление таких ограничений требует разработки новых подходов, например таких, которые предложены в рассматриваемом исследовании – комбинированное применение методов фаззинг-тестирования и символьной интерпретации.

Цель рассматриваемой работы заключается в повышении эффективности выявления дефектов программного обеспечения за счет разработки новых методов оптимизации предикатов пути, увеличивающих производительность символьной интерпретации, а также методы построения предикатов безопасности для ряда ошибок и их автоматизированного поиска.

Учитывая наличие нормативных требований по применению метода фаззинга и объективную потребность в повышении эффективности данного метода при испытаниях многочисленного программного обеспечения и средств защиты информации в рамках цикла безопасной разработки, актуальность проделанной работы сомнений не возникает.

Основные результаты

Результаты диссертационного исследования включают три положения, каждое из которых направлено на совершенствование отдельных показателей процедур выявления уязвимостей программного обеспечения.

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

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

В первой главе приведен подробный анализ состояния исследований по направлению работы с указанием достоинств и недостатков существующих решений, а также выводов с предложениями по их развитию.

Вторая глава посвящена описанию результатов по первому положению, выносимому на защиту, а именно – предложенному алгоритму слайсинга предиката пути, а также оценке его свойств.

В третьей главе представлено описание разработанного метода моделирования семантики ряда функций стандартной библиотеке с экспериментальной оценкой разработанного метода.

В четвертой главе представлены результаты по второму и третьему положениям, выносимым на защиту, а также результаты их практического применения и сравнение с существующими аналогами.

В пятой главе описаны результаты реализации разработанных методов в инструментальных средствах.

Заключение работы содержит краткое описание основных полученных результатов исследования.

Первое положение, выносимое на защиту, состоит в разработке алгоритма слайсинга предиката пути, применение которого повышает точность и скорость символьной интерпретации, используемой вместе с фаззинг-тестированием.

Второе положение, выносимое на защиту, состоит в разработке метода построения предиката безопасности для обнаружения некоторых типов ошибок.

Третье положение, выносимое на защиту, заключается в разработке метода автоматизированного поиска ошибок при помощи символьных предикатов безопасности во время динамического анализа.

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, 2 – в журналах, индексируемых в Web of Science и Scopus, а также 2 – сборниках докладов конференций. Зарегистрировано 2 программы для ЭВМ. Указанные результаты опубликованы в соавторстве с научным руководителем и другими авторами. Вместе с тем, грамотность изложения материала диссертации, единство и логическая взаимосвязь, полнота представленных результатов 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, дискретная математика, теории множеств и алгоритмов, теория компиляторов, анализа потока данных, 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 уточнении ограничений предиката пути, учитывающем зависимости переменных по данным, за счет чего устраняется избыточность предиката пути, что положительно влияет на производительность символьной интерпретации

Новизна второго положения, выносимого на защиту, заключается в применении методов символьной интерпретации и SMT-решателей для проверки наличия ошибок, для чего используется построение предиката безопасности, учитывающего особенности выполнения некоторых машинных инструкций, данных, содержащихся в ресурсах памяти ЭВМ.

Новизна третьего положения, выносимого на защиту, состоит в комбинированном применении методов фаззинга и символьной интерпретации, в том числе на основе результатов, полученных в первом и втором положениях, выносимых на защиту.

Теоретическая значимость работы состоит в разработке нового метода поиска ошибок нескольких типов, учитывающего особенности выполнения некоторых машинных инструкций, данных, содержащихся в ресурсах памяти ЭВМ, позволяющего в рамках использования гибридного фаззинга

эффективно находить соответствующие ошибки в программном обеспечении.

Практическая значимость полученных результатов подтверждается наличием 2 зарегистрированных программ для ЭВМ, соавтором которых является соискатель, реализующих предложенные методы и алгоритм, 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:

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

направлению исследований по пункту 5 – программные системы символьных вычислений.

Замечания

1. В работе не приводится анализ и оценка достаточности и избыточности ограничений предиката пути либо обоснования невозможности выполнения такого анализа.
2. На странице 33 в пункте 1.3.6 приводится категорическое утверждение "Производительность имеет решающее значение применительно к динамической символьной интерпретации", с которым трудно согласиться, поскольку основная цель все-таким – результативность поиска уязвимостей.
3. Метод моделирования семантики функции с точки зрения повышения производительности имеет смысл, однако адекватность моделирования в работе не оценивается, соответственно, влияние замены моделируемой функции на ее модель может снижать общую результативность поиска дефектов.
4. Из материалов работы не совсем понятна область применения предложенного алгоритма слайсинга предиката пути, а именно к программам какого объема и сложности он может быть применим, существуют ли ограничения по его применению, для программ, разработанных для каких аппаратных сред (процессорных архитектур) он может использоваться.

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 значения 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 двух 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 26.09.2022 года, предъявляемым к кандидатским диссертациям, а ее автор Вишняков Алексей Вадимович, заслуживает присуждения ученой степени кандидата физико-математических 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
"21" ноября 2022 г

Подпись Маркина Дмитрия Олег
Временно исполняющий обязанно
начальника кадрового аппарата П. Б. Севостьянов