

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук

Маркина Дмитрия Олеговича

на диссертационную работу Логуновой Влады Игоревны
по теме "Разработка методов гибридного фаззинга для приложений процессорных
архитектур Байкал-М и RISC-V 64",
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

Одним из наиболее эффективным методов поиска ошибок в программном обеспечении при реализации процедур разработки программного обеспечения является фаззинг-тестирование, при этом эффективность фаззинга зависит от применения методов символьной интерпретации в целях определения оптимальных корпусов входных данных с учетом сложности исследуемых программ и от поддержки процессорных архитектур аппаратных платформ, для которых исследуемые программы разработаны. Существенный интерес с точки зрения импортозамещения представляют аппаратные платформы на базе архитектуры процессоров RISC-V в виду ее открытости, а также с учетом специфики лицензирования – архитектура Байкал-М, разработанная на основе архитектуры ARM (AArch64). Указанными обстоятельствами обусловлена актуальность исследования методов гибридного фаззинга Логуновой В. И.

Цель рассматриваемой работы заключается в создании условий для обеспечения решения задачи символьной интерпретации бинарного кода программ, разработанных для аппаратных платформ на базе процессорных архитектур Байкал-М (AArch64) и RISC-V 64.

Применение символьной интерпретации при фаззинг-тестировании является обязательным требованием при поиске уязвимостей для программного обеспечения с высоким уровнем доверия.

Основные результаты

Результаты диссертационного исследования включают четыре положения, каждое из которых направлено на совершенствование процедур символьной интерпретации бинарного кода архитектур Байкал-М (AArch64) и RISC-V 64.

Диссертационная работа состоит из введения, пяти глав, заключения и списков литературы, рисунков, таблиц, алгоритмов, приложений и трех приложений.

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

Первая глава посвящена сравнительному описанию и анализу методов и инструментальных средств символьной интерпретации применительно к интерпретации программ для процессорных архитектур Байкал-М (AArch64) и RISC-V 64.

Во второй главе представлено описание разработанного метода динамической символьной интерпретации бинарного кода архитектуры Байкал-M (AArch64), включающего предложенные соискателем решения по моделированию символьного контекста для архитектуры AArch64, а также обнаружению косвенных переходов в бинарном коде.

В третьей главе представлены результаты разработки метода символьной интерпретации целочисленных инструкций архитектуры RISC-V в форме описания программной реализации данного метода в качестве библиотеки для фреймворка Triton.

Четвертая глава содержит описание разработанного метода динамической символьной интерпретации бинарного кода архитектуры RISC-V 64, включающего предложенные соискателем решения по моделированию символьного контекста для архитектуры RISC-V 64, предложения по доработке библиотеки DinamoRIO, решений по анализу табличных переходов.

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

Заключение работы содержит краткое описание основных полученных результатов исследования.

**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, 3 – в журналах, индексируемых в Web of Science и Scopus, а также зарегистрирована 1 программа для ЭВМ. Среди указанных научных работ одна опубликована соискателем с единоличным авторством, остальные – в соавторстве. В тексте автореферата имеются сведения с описанием вклада соискателя в совместные научные работы с другими авторами.

Грамотность изложения материала диссертации, единство и логическая взаимосвязь, полнота представленных результатов свидетельствуют о подготовке диссертации автором единолично и необходимым личным участием 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, выводов и рекомендаций,
сформулированных в диссертации, их достоверность, новизна и практическая
значимость**

Содержание исследования изложено на высоком научном уровне с применением новых научно обоснованных решений 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, в первую очередь методы символьной интерпретации и гибридного фаззинга применены соискателем корректно.

Полученные результаты по каждому положению, выносимому на защиту, сравнены с существующими аналогами. Показан положительный эффект от применения разработанных методов в совокупности. Указанные обстоятельства свидетельствуют о надлежащей *обоснованности* и *достоверности* полученных результатов.

Новизна первого положения, выносимого на защиту, состоит в разработке соискателем метода символьной интерпретации бинарного кода архитектуры AArch64. Автором описаны технические решения по моделированию символьного контекста и обнаружения косвенных переходов в бинарном коде архитектуры AArch64 в виде программной библиотеки для фреймворка Triton, что в совокупности позволяет применять метод символьной интерпретации в гибридном фаззинг-тестировании программ для аппаратных платформ на основе архитектуры процессоров AArch64.

Новизна второго положения, выносимого на защиту, заключается в разработке соискателем метода символьной интерпретации целочисленных инструкций архитектуры RISC-V, включая псевдо- и сокращенные инструкции.

Новизна третьего положения, выносимого на защиту, состоит в разработке метода символьной интерпретации бинарного кода архитектуры RISC-V 64, способного распознавать и анализировать косвенные ветвления даже в условиях ограниченной информации о списке инструкций базового блока.

Заявленное автором четвертое положение, состоящее, как заявлено в диссертации, в реализации методов, разработанных в первых трех положениях, выносимых на защиту, в инструменте Sydr, фактически содержит экспериментальную оценку эффективности данных методов и их сравнение с другими известными решениями, что, в свою очередь является обязательным критерием, которому должна отвечать диссертация.

Теоретическая значимость работы состоит в разработке новых методов символьной интерпретации бинарного кода для процессорных архитектур AArch64 и RISC-V 64, а также метода символьной интерпретации набора целочисленных инструкций RISC-V.

Практическая значимость полученных результатов подтверждается наличием 1 зарегистрированной программы для ЭВМ, соавтором которой является соискатель, реализующей 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:

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

Замечания

1. В работе не прослеживается специфика архитектуры Байкал-М по отношению к архитектуре ΛArch64, соответственно неочевидна целесообразность указания типа архитектуры Байкал-М как целевой для разработки метода динамической символьной интерпретации бинарного кода, не считая вопросов импортозамещения, которые в данном случае условны из-за зависимости от необходимости наличия лицензии на использование архитектуры ΛArch64 (ARM64), разработчиком и правообладателем которой является ARM Holdings – британская компания, резидент недружественной страны.

2. При реализации метода символьной интерпретации набора целочисленных инструкций и псевдоинструкций по содержанию автореферата и диссертации не удалось оценить полноту набора интерпретируемых инструкций относительно их общего количества, а также качество реализации инструкций.

3. Для некоторых реализаций программного обеспечения разработанный метод динамической символьной интерпретации бинарного кода процессорной архитектуры ΛArch64 не эффективен по сравнению с аналогами из-за отсутствия оптимизации при обработке большого массива входных данных в цикле.

4. Метод динамической символьной интерпретации бинарного кода процессорной архитектуры RISC-V 64 для случаев наличия больших циклов в анализируемом коде не учитывает уже исследованные итерации, из-за чего анализ занимает больше времени.

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 символьной интерпретации.

Заключение о соответствии 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 изложены научно обоснованные технические решения и разработки, имеющие существенное значение для развития страны, в области совершенствования процессов разработки безопасного программного обеспечения, применяемого в критической информационной инфраструктуре.

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 одной программы для ЭВМ. Присутствуют сведения о внедрении программы и эксплуатации в программных системах ИСИ РАН, а также процессах разработки

безопасного программного обеспечения ООО "Фобос-ИТ" и ООО "Лаборатория безопасности".

Предложенные автором диссертации решения аргументированы и оценены по сравнению с другими известными решениями.

Основные научные результаты опубликованы в рецензируемых научных изданиях: соискателем опубликовано 5 научных работ и получено 1 свидетельство о государственной регистрации программы для ЭВМ, из них 3 научных статьи в периодических научных журналах с индексацией Web Of Science и Scopus, и 2 -- в журналах, включенных в перечень рецензируемых научных изданий ВАК при Минобрнауки РФ.

Рецензируемые научные издания, в которых опубликованы основные результаты диссертации, соответствуют требованиям, установленным Минобрнауки РФ.

Количество публикаций, в которых излагаются основные научные результаты диссертации на соискание ученой степени кандидата наук, соответствует требуемому.

При использовании заимствованных материалов и отдельных результатов соискатель в диссертации корректно приводит ссылки на автора и(или) источник заимствования, а также отмечает степень участия в качестве автора (лично и(или) в соавторстве) при использовании собственных результатов научных работ.

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 16.10.2024 года, предъявляемым к кандидатским диссертациям, а ее автор Логунова Влада Игоревна, 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 ФГКВООУ ВО "Академия Федеральной службы охраны
Российской Федерации"

кандидат технических наук

Д. О. Маркин

" 26 " 11 2025 г

Подпись Маркина Дмитрия Олеговича ЗАВЕРЯЮ

Начальник кадрового аппарата

А. Б. Семибратов