

«УТВЕРЖДАЮ»
Директор Федерального
государственного учреждения
«Федеральный исследовательский
центр «Информатика и управление»
Российской академии наук»,
член-корреспондент РАН

___ М.А.Посыпкин

«24» 11 2025 г.

МП

ОТЗЫВ

ведущей организации – Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук» (ФИЦ ИУ РАН) – на диссертационную работу Логуновой Влады Игоревны «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

Диссертационная работа В. И. Логуновой посвящена развитию методов анализа программного обеспечения процессорных RISC-архитектур Байкал-М и RISC-V 64. Применение автоматизированного фаззинг-тестирования в виде множественных запусков исследуемой программы с различными входными данными позволяет выявлять и устранять программные дефекты и уязвимости в рамках жизненного цикла разработки безопасного ПО. Гибридный фаззинг, представляющий собой сочетание мутационного фаззинг-тестирования и динамической символьной интерпретации, обеспечивает не только высокую производительность, но и аналитическую точность для выявления зависимостей поведения программы от полученных извне входных данных. При подобном тестировании с помощью символьных методов анализа увеличивается вариативность исследуемых путей исполнения и, соответственно, пространство поиска программных ошибок. Согласно проведенному в работе анализу, подавляющее большинство современных символьных анализаторов бинарного кода способно исследовать приложения только для архитектуры x86/x86_64. В то же время довольно распространенными энергоэффективными RISC-архитектурами, пригодными для широкого ряда применений и, в том числе, задач импортозамещения являются Байкал-М (ARM/AArch64) и RISC-V. В диссертационной работе В. И. Логуновой предлагаются новые методы

динамической символьной интерпретации бинарного кода для архитектур Байкал-М и RISC-V 64. Методы поддерживают возможность символьного анализа косвенной адресации и обладают практической применимостью в контексте гибридного фаззинга. Таким образом, тема диссертационной работы В. И. Логуновой является актуальной.

Структура и основное содержание диссертационной работы

Диссертация имеет общий объём 117 страниц и состоит из введения, пяти глав, заключения и списка литературы из 91 источника.

Во введении описывается актуальность темы исследования, формируются цель и задачи диссертационной работы, указывается научная новизна полученных результатов и раскрывается их теоретическая и практическая значимость, приводятся основные положения, выносимые на защиту.

В первой главе приводится обзор работ по теме диссертации, а также рассматриваются основные принципы работы, оптимизации и техники анализа символьных данных. Приводится описание существующих инструментов динамической символьной интерпретации в контексте их применимости для различных архитектур и в рамках гибридного фаззинг-тестирования.

Вторая глава посвящена предлагаемому методу динамической символьной интерпретации бинарного кода архитектуры Байкал-М (AArch64), основанному на конкретно-символьном подходе с применением динамической бинарной инструментации. В главе выделяется набор архитектурно-зависимых компонентов, требуемых для проведения динамической символьной интерпретации на уровне бинарного кода, а также освещаются отличительные аспекты такого анализа для архитектуры Байкал-М (AArch64). Далее раскрывается используемый в предлагаемом методе механизм разрешения косвенных табличных переходов (switch-выражений) и способ определения размеров соответствующей таблицы в исполняемом коде при помощи анализа предыдущего базового блока программы.

В третьей главе представлен разработанный метод символьной интерпретации набора целочисленных инструкций архитектуры RISC-V, включающего сокращенные инструкции и псевдоинструкции. В главе описываются границы применимости предлагаемого метода с точки зрения поддерживаемых расширений инструкций, а именно RV64IMC и RV32IMC, после чего рассматриваются детали реализации метода в модуле разрешения архитектурных зависимостей открытой символьной библиотеки Triton. В том числе, приводится описание особенностей конструирования символьных выражений для операционной семантики псевдоинструкций и сокращенных инструкций. В качестве демонстрации практической применимости предложенного метода рассматривается реализованная на его основе символьная эмуляция для задачи захвата флага (CTF).

В четвертой главе обсуждается разработанный метод динамической символьной интерпретации бинарного кода архитектуры RISC-V 64, который в рамках осуществления конкретно-символьного анализа посредством инструмента Sydr, опирается на метод, представленный в третьей главе. В главе приводится краткая характеристика описываемого метода и набора

соответствующих компонентов архитектуры RISC-V 64. Далее рассматриваются потребовавшиеся в процессе реализации метода изменения в работе динамического бинарного инструментатора и алгоритм анализа косвенных табличных переходов в условиях неполной информации о списке инструкций текущего исполняемого базового блока.

Пятая глава содержит экспериментальную оценку разработанных методов динамической символьной интерпретации для процессорных архитектур Байкал-М (AArch64) и RISC-V 64. При сравнении реализации предложенных методов в символьном интерпретаторе Sydr с его открытым аналогом SymQEMU для набора реальных приложений, разработанные методы демонстрируют лучшие показатели с точки зрения метрики достигнутого покрытия для обеих целевых архитектур. Помимо этого, при применении методов в контексте гибридного фаззинга наблюдается улучшение показателей покрытия по сравнению с мутационным фаззинг-тестированием: для архитектуры Байкал-М на 10 из 12 проектов при сравнении с инструментом libFuzzer и на 8 из 12 проектов при сравнении с AFL++; для архитектуры RISC-V 64 на 3 из 4 проектов при сравнении с инструментом libFuzzer. Результаты демонстрируют состоятельность предложенных методов и их практическую применимость в гибридном фаззинге.

В заключении сформулированы основные результаты диссертации.

Основные результаты диссертационной работы

В диссертационной работе В. И. Логуновой получены следующие основные результаты:

1. Разработан метод динамической символьной интерпретации бинарного кода программ архитектуры Байкал-М (AArch64).
2. Разработан метод символьной интерпретации набора целочисленных инструкций архитектуры RISC-V, включающего сокращенные инструкции и псевдоинструкции.
3. Разработан метод динамической символьной интерпретации бинарного кода программ архитектуры RISC-V 64.
4. Реализованы алгоритмы определения возможных направлений косвенных переходов для бинарного кода архитектур Байкал-М (AArch64) и RISC-V 64.
5. Разработанные методы были реализованы в инструментах Triton и Sydr, а также была проведена оценка их эффективности.

Основные результаты диссертации были представлены на профильных научных конференциях и отражены в 5 статьях, в том числе, двух – опубликованных в изданиях из перечня ВАК, трех – в журналах Web of Science и Scopus. Помимо этого, получено 1 свидетельство о регистрации программы для ЭВМ.

Теоретическая и практическая значимость полученных результатов

Теоретическая значимость работы заключается в разработанных методах динамической символьной интерпретации бинарного кода процессорных архитектур Байкал-М (AArch64) и RISC-V 64, а также методе символьной интерпретации набора целочисленных инструкций RISC-V на основе конструирования абстрактных синтаксических деревьев их операционной семантики. Кроме того, для вышеуказанных архитектур была проведена экспериментальная оценка эффективности применения методов динамической символьной интерпретации в контексте фаззинг-тестирования.

Практическая значимость работы заключается в том, что предложенные методы анализа бинарного кода архитектур Байкал-М (AArch64) и RISC-V 64 были реализованы в разрабатываемом ИСП РАН инструменте динамической символьной интерпретации Sydr, входящем в фреймворк гибридного фаззинга Sydr-Fuzz. В рамках данных инструментов предложенные методы применяются в Центре доверенного искусственного интеллекта ИСП РАН, а также они были внедрены в процессы безопасной разработки ООО "Фобос-НТ" и ООО "Лаборатория безопасности". Метод символьной интерпретации набора целочисленных инструкций архитектуры RISC-V, включающего сокращенные инструкции и псевдоинструкции, был интегрирован в открытую символьную библиотеку Triton, доступную широкому кругу исследователей безопасности программного обеспечения.

Рекомендации по использованию результатов.

Результаты, которые получены в диссертационной работе, могут лечь в основу методов, поддерживающих архитектурно-зависимые компоненты для отслеживания преобразований символьного контекста при выполнении программ. Разработанные для указанных архитектур методы могут быть применимы к бинарным программам, работающим под управлением ОС Linux.

Кроме того, результаты диссертации могут быть использованы в учебном процессе студентов МИЭТ, РТУ МИРЭА, МГТУ им. Н.Э. Баумана, МФТИ, МИФИ и других технических вузов и университетов при изучении инструментов динамического анализа программного кода, а также в научно-исследовательской деятельности – в ФИЦ ИУ РАН, Института программных систем им. А.К. Айламазяна, Санкт-Петербургского института информатики и автоматизации и других организациях.

Замечания по работе

Несмотря на общую положительную оценку при рассмотрении диссертационной работы выявлен ряд замечаний:

1. Недостаточно подробно раскрыты способы определения размеров таблиц косвенных переходов в бинарном коде (главы 2 и 4).

2. Не приводится анализ и оценка достаточности набора используемых расширений архитектуры RISC-V в главе 3.

3. Не приводится сравнение гибридного фаззинга со вторым инструментом мутационного фаззинга (AFL++) для архитектуры RISC-V 64, используемого в аналогичном сравнении для архитектуры Байкал-М, либо обоснование невозможности провести такое сравнение.

Отмеченные недостатки не снижают положительной оценки рецензируемой диссертационной работы.

Заключение по работе

Диссертация В. И. Логуновой является законченной научно-квалификационной работой, в которой решена актуальная задача разработки методов гибридного фаззинга для приложений процессорных архитектур Байкал-М и RISC-V 64. Диссертация соответствует паспорту научной специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (пп. 1, 2). Основные результаты диссертации в достаточной мере апробированы на профильных конференциях и отражены в публикациях, в том числе, в изданиях из перечня ВАК. Содержание диссертационной работы корректно отражено в автореферате.

Таким образом, диссертационная работа В. И. Логуновой полностью соответствует требованиям ВАК РФ, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук, а её автор, Логунова Влада Игоревна, заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Отзыв ведущей организации обсужден и принят на заседании секции Ученого Совета Федерального государственного учреждения "Федеральный исследовательский центр "Информатика и управление" Российской академии наук" 24 ноября 2025 года, протокол № 7.

Заместитель директора ФИЦ ИУ РАН
по научной работе, д.ф.-м.н.

Разумчик Р.В.

Руководитель Отделения ФИЦ ИУ РАН,
главный научный сотрудник, д.ф.-м.н.

Синицин В.И.

Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" Российской академии наук" (ФИЦ ИУ РАН)

Адрес: 119333, г. Москва, ул. Вавилова, 44, к.2.

Сайт: <https://www.frccsc.ru/>

Тел.: +7(499) 135-62-60

Эл.почта: frccsc@frccsc.ru