ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Логуновой Влады Игоревны

«Разработка методов гибридного фаззинга для приложений процессорных архитектур Байкал-М и RISC-V 64», представленную на соискание ученой степени кандидата технических наук по

специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертационная работа Логуновой В. И. посвящена разработке новых методов динамической символьной интерпретации для возможности проведения гибридного фаззинг-тестирования приложений процессорных архитектур Байкал-М (AArch64) и RISCV64. Методы должны быть применимы к бинарным программам, работающим под управлением ОС Linux, и не требовать доступности исходного кода.

Для создания качественного и безопасного ПО необходимы автоматизированные средства тестирования, позволяющие выявлять и устранять программные ошибки и уязвимости. К таким средствам относятся инструменты динамического анализа, включающие методы фаззинга с обратной связью по покрытию и динамическую символьную интерпретацию. При совместном применении в виде гибридного фаззинга эти подходы демонстрируют увеличение результативности анализа благодаря взаимодополняющей комбинации скорости мутационного фаззинга и способности символьной интерпретации к обнаружению специфических и граничных условий. Важным аспектом для промышленного применения инструментов динамической символьной интерпретации является возможность исследовать бинарный код, что приводит к потребности в универсальных кроссплатформенных решениях. В то время как происходит активное развитие кодовой базы архитектур AArch64 и RISC-V, большинство современных динамических символьных интерпретаторов ориентировано на анализ приложений архитектуры x86/x86_64. Немногие из данных инструментов способны проводить анализ для архитектуры ARM/AArch64. Для 64-битных приложений открытой архитектуры RISC-V подобных решений найти не удалось. Перечисленные факторы делают работу Логуновой В. И. особенно актуальной.

В рамках подготовки диссертации Логунова В. И. системно и методично решала поставленные задачи. Ею был разработан метод символьной интерпретации набора целочисленных инструкций архитектуры RISC-V, реализованный в открытом инструменте Triton. Разработанный метод также включает интерпретацию наборов сокращенных инструкций и псевдоинструкций. Также были разработаны методы динамической символьной

интерпретации бинарного кода программ архитектур Байкал-М и RISCV64. Оба метода позволяют обнаруживать в машинном коде косвенные условные переходы и определять для них границы таблиц переходов с целевыми адресами для передачи управления. Предложенные методы динамической символьной интерпретации были реализованы в инструменте Sydr, который разрабатывается в ИСП РАН и входит в комплекс гибридного фаззинга Sydr-Fuzz. Экспериментальное сравнение реализованных в инструменте Sydr методов с открытым аналогом SymQEMU для наборов прикладных программ обеих архитектур показало увеличение достигнутой метрики покрытия кода при использовании разработанных методов. Также в ходе экспериментов с использованием фреймворка тестирования FuzzBench было показано преимущество гибридного фаззинга (один поток фаззинга и один поток символьной интерпретации) по сравнению с двумя потоками фаззинга.

Таким образом, разработанные Логуновой В. И. методы динамической символьной интерпретации продемонстрировали свою эффективность, и могут быть использованы для проведения гибридного фаззинг-тестирования кода программ Байкал-М и RISCV64. Кроме того, метод интерпретации инструкций RISC-V может быть использован сообществом разработчиков для создания новых инструментов динамического анализа для данной архитектуры.

Полученные Логуновой В. И. результаты были опубликованы в авторитетных изданиях и обсуждались на конференциях.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК РФ к работам на соискание ученой степени кандидата технических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а её автор, Логунова Влада Игоревна, заслуживает присуждения ему учёной степени кандидата технических наук.

Научный руководитель: с.н.с. ИСП РАН, к.ф.-м.н. Гетьман А.И.

5 октября 2025 года