ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Куца Даниила Олеговича

«Метод моделирования косвенной адресации в рамках динамической символьной интерпретации», 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 Куца Д.О. посвящена разработке нового метода моделирования косвенной адресации в рамках динамической символьной интерпретации. Метод должен быть применим к бинарным программам, работающим под управлением ОС Linux, и не требовать доступности исходного кода.

Развитие современного общества невозможно представить без использования вычислительной техники и программного обеспечения. Кодовая база программных продуктов растёт, активно используются решения с открытым исходным кодом, и, как следствие растёт количество ошибок и уязвимостей. Обычные бытовые предметы (холодильники, чайники, стиральные машины и т. д.), входящие в состав «умного дома» могут обрабатывать конфиденциальную информацию и иметь доступ в интернет. Всё это открывает широкий простор для действий злоумышленников.

При промышленной разработке программного обеспечения активно применяется безопасный цикл разработки ПО (SDL) для поиска ошибок и уязвимостей. Применение инструментов анализа кода разработчиками повышает качество и безопасность разрабатываемых продуктов, позволяя находить ошибки на стадии разработки. Статический и динамический анализ являются общеизвестными подходами к поиску ошибок. Одним из наиболее часто используемых подходов к динамическому анализу является фаззинг с обратной связью по покрытию кода.

Комбинирование различных методов динамического анализа, а именно методов фаззинга и динамической символьной интерпретации активно изучается исследователями в мировом сообществе. В такой комбинации динамическая символьная интерпретация призвана обеспечить обнаружение сложных состояний программы, труднодоступных для классического фаззинга с обратной связью. Существующие инструменты, реализующие методы динамической символьной интерпретации учитывают только явные зависимости по данным. Это накладывает ограничение на моделирование передачи управления с косвенной адресацией и обработку любых табличных преобразований, что в совокупности приводит к снижению эффективности применения символьной интерпретации в комбинации с фаззингом. Все эти факторы делают работу Куца Д.О. крайне актуальной.

В рамках подготовки диссертации Куц Д.О. системно и методично решал поставленные задачи. Им был разработан метод поиска и моделирования косвенных переходов, позволяющий обнаруживать такие конструкции в бинарном коде и определять целевые адреса переходов. Для определения границ таблицы переходов используется

разработанный эвристический подход, основанный на анализе содержимого таблицы. Также был разработан метод моделирования чтений памяти по символьно вычисляемому адресу, который позволяет учитывать косвенную адресацию в символьной модели исполнения программы. Предложенные методы реализованы в инструменте динамической символьной интерпретации Sydr, который разрабатывается в ИСП РАН. Экспериментальная оценка метода на наборе прикладных программ показала, что предложенные методы позволяют увеличить число инвертируемых символьных условных переходов и достичь большего покрытия по коду в рамках анализа.

Таким образом, разработанные Куцом Д.О. методы показали свою эффективность и могут быть использованы в рамках комбинации методов символьной интерпретации и фаззинга.

Полученные диссертантом 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, Куц Даниил Олегович, заслуживает присуждения ему учёной степени кандидата технических наук.

Научный руководитель: с.н.с. ИСП РАН, к.т.н. Федотов А.Н.

27 июля 2023 года