ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Вишнякова Алексея Вадимовича

«Поиск ошибок в бинарном коде методами динамической символьной интерпретации», представленную на соискание ученой степени кандидата физико-математических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертационная работа Вишнякова А.В. посвящена разработке нового метода поиска ошибок в бинарном коде методами динамической символьной интерпретации. Метод должен иметь возможность применения в контексте гибридного фаззинга, сочетающего в себе динамическую символьную интерпретацию и фаззинг с обратной связью по покрытию.

С развитием современного программного обеспечения происходит неизбежный рост кодовой базы, и, как следствие растёт количество ошибок и уязвимостей. Вычислительная техника всё глубже проникает в повседневную жизнь. Активно развиваются технологии «умного дома» и «интернета вещей», даже обычные бытовые предметы (чайники, холодильники, кондиционеры и т. д.) могут обрабатывать конфиденциальную информацию и быть подключены к сети интернет. Безусловно, это расширяет поверхность атаки и пространство для действий злоумышленников.

Безопасный цикл разработки ПО (SDL) применяется лидерами индустрии и фактически становится отраслевым стандартом для обнаружения ошибок и уязвимостей непосредственно во время процесса разработки программного обеспечения. Разработчики применяют различные инструменты анализа кода для повышения безопасности и качества разрабатываемых продуктов, что позволяет обнаруживать ошибки на ранней стадии, ещё до ввода в эксплуатацию. Поиск ошибок производится широко известными методами статического и динамического анализа. Фаззинг является одним из основных методов динамического анализа, который применяется во время безопасного цикла разработки программного обеспечения. Современные методы фаззинга учитывают обратную связь по покрытию кода. При таком подходе осуществляется наблюдение не только за результатом выполнения исследуемой программы, но и собирается информация о покрытых участках кода программы. Обратная связь основана на использовании генетических алгоритмов.

В научной среде последние годы активно обсуждается вопрос комбинации методов фаззинга и динамической символьной интерпретации. Применение динамической символьной интерпретации в рамках такого гибридного подхода позволяет решать следующие задачи: обнаруживать сложные состояния программы, труднодоступные для классического фаззинга с обратной связью, а также целенаправленный поиск ошибок. Существующие подходы к поиску ошибок методами символьной интерпретации либо работают на уровне исходного кода, либо используют статический анализ, а также часто сосредотачиваются на поиске одного конкретного типа ошибок. Некоторые представленные решения недоступны для использования. Все эти факторы делают работу Вишнякова А.В. крайне актуальной.

В рамках подготовки диссертации Вишняков А.В. методично и системно решал поставленные задачи. Им был разработан алгоритм слайсинга предиката пути, который позволяет устранять избыточные ограничения во время динамической символьной интерпретации бинарного кода. Алгоритм основан на анализе зависимостей символьных переменных по данным. Данный алгоритм позволяет повысить точность генерации входных данных с помощью символьной интерпретации, что непосредственно влияет на обнаружение ошибок. Также был разработан метод построения предикатов безопасности для обнаружения ошибок деления на нуль, целочисленного переполнения и выхода за границы массива во время динамической символьной интерпретации. Экспериментальная оценка метода на наборе тестов Juliet показала общую точность 95.59% для 11 классов ошибок CWE (15772 теста). Разработан автоматизированный метод поиска ошибок при помощи символьных предикатов безопасности во время динамического анализа программ на корпусе входных файлов, полученного в результате гибридного фаззинга. Предложенный метод позволил обнаружить 17 новых ошибок в 10 различных проектах с открытым исходным кодом. Таким образом, разработанные Вишняковым А.В. методы показали свою эффективность и могут быть использованы в рамках безопасного цикла разработки программного обеспечения.

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 физико-математических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а её автор, Вишняков Алексей Вадимович, заслуживает присуждения ему учёной степени кандидата физико-математических наук.

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

10 октября 2022 года