Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук
Маркина Дмитрия Олеговича
на диссертационную работу Шимчика Никиты Владимировича
по теме "Исследование и разработка методов поиска уязвимостей
в программах на C и C++ на основе статического анализа
помеченных данных",
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

Развитие цифровой экономики неизбежно определяется ростом количества и объема кодовой базы разрабатываемого программного обеспечения. Безопасность программного обеспечения определяется многочисленными факторами, среди которых наиболее важны применяемые на всех этапах жизненного цикла разработки безопасного программного обеспечения методов и средств по выявлению и устранению уязвимостей и дефектов программного обеспечения. Рост объема и сложности программного обеспечения усложняет применение различных методов поиска и выявление дефектов и уязвимостей и требует разработки новых подходов. К перспективным направлениям поиска дефектов программного кода относятся методы на основе помеченных данных, позволяющие обнаруживать дефекты и уязвимости, связанные с получением данных из недоверенных источников, либо отслеживать потенциальные утечки защищаемых данных. Совершенствованию таких методов посвящена рассматриваемая работа, что определяет ее актуальность для развития методов анализа безопасности программного обеспечения.

Основные результаты

Результаты диссертационного исследования включают четыре положения, каждое из которых направлено на повышение полноты и точности выявления уязвимостей методом статистического анализа помеченных данных.

Диссертационная работа состоит из введения, пяти глав, заключения и списка литературы.

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

Первая глава посвящена анализу современных методов поиска уязвимостей, при этом особое внимание уделено символьной интерпретации,

анализу помеченных данных, а также особенностях современных реализации данных методов, достоинств и недостатков известных технических решений.

Во второй главе представлено описание предложенного автором алгоритма снятия помеченности с целочисленных переменных, позволяющего сократить количество ложных срабатываний при выполнении статического анализа, а также описание метода проверки реализуемости (неконсистентности) пути в программе на основе двухэтапного анализа

В третьей главе описывается алгоритм вычисления множества кандидатов для вызовов в случаях, когда в программе функции вызываются по указателю (выполняется косвенный вызов), позволяющий повысить результативность поиска вызываемых функций, в том числе за счет использования дополнительных эвристических особенностей работы алгоритма.

В четвертой главе автором предложен алгоритм, повышающий эффективность распространения помеченной глобальной переменной.

Пятая глава посвящена описанию разработанного автором инструментального средства, реализующего предложенные алгоритмы.

Заключение работы содержит краткое описание основных полученных результатов исследования.

Первое положение, выносимое на защиту, состоит в разработке алгоритма анализа косвенных вызовов, позволяющего найти информацию о возможных кандидатах для вызова по указателю на основе межпроцедурного анализа потока данных IFDS.

Второе положение, выносимое на защиту, состоит в разработке алгоритма снятия помеченности с целочисленных переменных, значение которых было проверено, применимый в нечувствительном к путям анализе.

Третье положение, выносимое на защиту, состоит в разработке алгоритма направленного распространения помеченности через глобальные переменные, позволяющий не исследовать функции, которые не зависят от значения этих переменных.

Четвертое положение, выносимое на защиту, состоит в разработке метода проверки реализуемости пути в программе на основе двухэтапного анализа.

Личное участие соискателя ученой степени в получении результатов, изложенных в диссертации, полнота изложения материалов диссертации в работах, опубликованных соискателем

Соискателем по теме работы опубликовано 4 научных статьи в журналах, рекомендованных ВАК, а также 2 статьи, индексируемых в Web of Science и Scopus. Зарегистрировано 5 программ для ЭВМ.

Статьи подготовлены и опубликованы соискателем в соавторстве с научным руководителем и другими авторами. Результаты апробировались на достаточном количестве открытых конференций всероссийского и международного уровня. Представленные результаты свидетельствуют

о подготовке диссертации автором единолично и необходимом личном участии 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, достоверность результатов, их новизна и практическая значимость

Содержание исследования изложено на высоком научном уровне с применением оригинального подхода 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, графов и алгоритмов, а также методы статического анализа программ, символьной интерпретации применены соискателем корректно. Полученные результаты по каждому положению, выносимому на защиту, сравнены с существующими аналогами, показан положительный эффект от их применения. Указанные обстоятельства свидетельствуют о надлежащей *обоснованности* и *достоверности* полученных результатов.

Новизна первого положения, выносимого на защиту, состоит в решении задачи достижимости по межпроцедурно реализуемым путям на расширенном суперграфе при поиске кандидатов для вызовов по указателю (косвенных вызовов функций), позволяющей повысить результативность поиска кандидатов.

Новизна второго положения, выносимого на защиту, заключается в использовании сравнительно простой эвристики, основанной на проверке безопасности целочисленных данных для заданных условий, позволяющей снизить количество ложных срабатываний.

Новизна третьего положения, выносимого на защиту, состоит в использовании дополнительных сведений, предоставляемых инфраструктурой LLVM, в целях сокращения неоправданного распространения помеченности глобальных переменных и повышения оперативности анализа в целом.

Новизна четвертого положения, выносимого на защиту, состоит в использовании двухэтапного анализа, использующего три дополнительных

введенных автором критерия консистентности пути в целях сокращения количества ложных срабатываний.

Теоретическая значимость работы состоит в разработке новых алгоритмов анализа помеченных данных, позволяющих при выполнении статического анализа сократить время анализа и количество ложных срабатываний анализатора.

Практическая значимость полученных результатов подтверждается наличием 5 зарегистрированных программ для ЭВМ, соавтором которых является соискатель, реализующих предложенные алгоритмы, 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 направлениям исследований по пункту 1 – модели, методы и алгоритмы проектирования, анализа, трансформации, верификации и тестирования программ и программных сетей.

Замечания

1. При решении задачи определения вызываемой функции при использовании вызовов по указателю (косвенных вызовов) для повышения полноты анализа предложено использовать метод вычисления множества кандидатов для вызовов по указателю на основе метода IFDS с ограничением по времени и глубине. Несмотря на использование предложенной дополнительной эвристической для оптимизации поиска характеристики, учет заданных ограничений не позволит провести полный анализ.

2. Предложенная эвристика на основе названия функции и типах ее аргументов, используемая для поиска потенциальных истоков помеченных данных, достаточно условна и позволяет получать положительный эффект от ее применения на ограниченном количестве объектов оценки.

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 и алгоритмов анализа, верификации и тестирования программ и программных систем.

Заключение о соответствие 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 содержится решение научной задачи, имеющей значение для развития соответствующей отрасли знаний.

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 пяти программ для ЭВМ. Присутствуют сведения об их эксплуатации в программных системах ИСП РАН.

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 25.01.2024 года, предъявляемым к кандидатским диссертациям, а ее автор Шимчик Никита Владимирович, 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 ФГКВОУ ВО "Академия Федеральной службы охраны Российской Федерации"
кандидат технических наук Д. О. Маркин
"28" мая 2024 г.