врио Ди
государ
«Федеральный
исследовательск
исследований Росс
(Ф
д. т. н. Вла

15 февраля 2019

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу

Асланяна Айка Кареновича

«Методы статического анализа для поиска дефектов в исполняемом коде программ», представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Актуальность

Несмотря на тенденцию расширения сфер применения открытого программного обеспечения, во многих системах используются проприетарный код, а также библиотеки в виде перекомпилированных бинарных модулей, которые по разным причинам могут долгое время не обновляться. Подобный код необходимо проверять на ошибки, поскольку дефекты в нем могут повлиять как на весь программный продукт в целом, так и на безопасность его применения. Так, дефекты в программном обеспечении объектов критической информационной инфраструктуры (например, автоматизированных систем управления медицинским оборудованием, транспортными потоками, объектами химического производства и т.п.) могут представлять опасность жизни и здоровью людей.

Увеличение размера программ осложняет поиск дефектов вручную, поэтому требуются методы, позволяющие автоматизировать поиск ошибок в бинарном коде. Одним из подходов к автоматическому поиску дефектов является статический анализ кода. Поиск ошибок с помощью статического анализа имеет определенные преимущества: можно провести одновременный анализ нескольких путей выполнения, а также поиск ошибок на редко исполняемых путях, которые могут быть не покрыты тестами при динамическом анализе. Вместе с тем статические анализаторы выдают ложные срабатывания, т. е. предупреждения, которые описывают ситуации в коде, не являющиеся ошибочными.

Диссертационная работа Асланяна А. К. посвящена исследованию и разработке методов статического анализа для поиска дефектов в исполняемом коде программ. В настоящий момент существует ряд инструментов статического анализа, но большинство из них разработаны для анализа исходного кода. Вместе с тем, для полноценного анализа таких инструментов недостаточно ввиду того, что исходный код может быть доступен лишь частично. Требуются методы и средства статического анализа, позволяющие производить поиск дефектов в бинарном коде программ и библиотек, что обуславливает актуальность диссертационной работы Асланяна А. К. в отношении как теории, так и практики программирования.

Общая характеристика работы

Диссертационная работа состоит из введения, четырех глав основного содержания, заключения и приложения. Полный объем диссертации составляет 118 страниц, включая 11 рисунков и 22 таблицы. Список литературы содержит 89 наименований.

Во введении описывается актуальность исследуемой предметной области, формулируется цель и ставится задача диссертационной работы, указываются актуальность, научная новизна и практическая значимость полученных результатов исследования, формулируются основные положения, выносимые на защиту.

В первой главе приводится обзор работ, которые имеют отношение к теме диссертации. Рассматриваются современные методы анализа исполняемого кода,

поиска клонов исполняемого кода, сравнения двух версий исполняемых файлов. Перечисляются преимущества и недостатки каждого метода.

Вторая глава посвящена архитектуре предлагаемого инструмента. Приводится описание применения абстрактной интерпретации и анализа потока данных для анализа исполняемых файлов, а также используемой модели памяти для ячеек в стеке, в динамической и в статической памяти. В предлагаемом подходе исполняемый код переводится в архитектурно-независимое промежуточное представление, после чего применяется анализ значений, помеченных данных, достигающих определений и т.д. Все виды анализа являются межпроцедурными, контекстно-чувствительными и потоко-чувствительными. Кроме того, разработанная архитектура позволяет добавлять новые виды анализа.

В третьей главе рассматриваются предложенные методы поиска клонов исполняемого кода, сравнения исполняемых файлов и анализа характера изменений между двумя версиями программы. Поиск клонов проводится с использованием графов зависимостей программы, что позволяет достичь высокой точности. При сравнении исполняемых файлов сопоставляются функции одного исполняемого файла с функциями второго исполняемого файла на основе графов зависимостей программы и графов вызовов функций. Анализ характера изменений между двумя версиями программы проводится с использованием результата сравнения исполняемых файлов.

В четвертой главе приводится описание поиска дефектов использования памяти после освобождения, форматных строк, переполнений буферов, внедрения команд. Предлагается метод поиска неисправленных частей в новых версиях программ.

В заключении формулируются основные результаты диссертационной работы и направления дальнейших исследований.

Результаты, полученные в диссертационной работе, соответствуют поставленной цели и сформулированным задачам. Содержание диссертации соответствует требованиям специальности 05.13.11. Текст диссертации и автореферата оформлены в соответствии с требованиями, предъявляемым к

диссертационным работам. Автореферат объективно отражает содержание диссертационной работы.

Основные результаты диссертационной работы

1. Разработана архитектура инструмента статического анализа исполняемого кода.
2. Предложены и разработаны методы анализа значений и помеченных данных, позволяющие проводить межпроцедурный, чувствительный к контексту, к потоку данных и к потоку управления анализ.
3. Предложены и разработаны методы поиска клонов исполняемого кода и сравнения двух версий исполняемых файлов для автоматического поиска и определения характера изменений в новых версиях программ.
4. Предложены и разработаны методы поиска дефектов использования памяти после освобождения, двойного освобождения памяти, переполнения буфера, форматных строк и внедрения команд, а также поиска неисправленных фрагментов в новой версии исполняемого файла.

По диссертации могут быть сделаны следующие **замечания**:

1. В тексте автореферата присутствуют опечатки, ряд утверждений автора имеют выраженный эмоциональный оттенок
2. Не приводятся результаты сравнения предлагаемой во второй главе архитектуры инструмента статического анализа с известными аналогами.

Заключение

Указанные замечания не влияют на общую положительную оценку диссертационной работы. Результаты диссертации, полученные Асланяном А. К., обладают научной новизной и практической ценностью, а сама диссертационная работа может быть квалифицирована как законченное научное исследование по актуальной тематике.

Анализ основных результатов работы позволяет сделать заключение о соответствии диссертационной работы требованиям, предъявляемым ВАК РФ к

работам на соискание степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Отзыв на диссертацию обсуждён на научно-исследовательском семинаре «Высокопроизводительные вычислительные системы и их применение» Межведомственного суперкомпьютерного центра Российской академии наук - филиала Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» 15 февраля 2019 года, протокол № 2.

заместитель директора по научной работе –
директор МСЦ РАН – филиала
ФГУ ФНЦ НИИСИ РАН
к.т.н., доцент Шабанов
Борис Михайлович