ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

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

В современном мире программное обеспечение используется повсеместно, начиная с мобильных телефонов и заканчивая различными системами управления предприятий и медицинским оборудованием. Между тем, исходный код часто либо не доступен для анализа, либо доступен лишь частично, поэтому требуются методы и инструменты позволяющие осуществлять поиск дефектов непосредственно в исполняемом коде программ. Другая причина обуславливающая потребность в таком инструменте, поиск дефектов, по различным причинам, проявляющихся только в исполняемом коде программ - например, из за агрессивных оптимизаций компилятора. Целью диссертационной работы Асланяна А.К. является исследование и разработка методов статического анализа исполняемого кода для поиска дефектов. Методы должны быть архитектурно независимыми, обладать высокой точностью и масштабируемостью для анализа исполняемых файлов размером в десятки мегабайт (несколько миллионов строк исходного кода) за несколько часов, а также обладать высокой точностью (количество правильных срабатываний − больше 50%) и расширяемостью для поиска новых типов дефектов.

Актуальность выбранной темы обеспечивается тем, что в мире существует всего несколько коммерческих анализаторов, отвечающих заданным критериям и их код закрыт, а о используемых методах и алгоритмах детально не известно. Тем не менее, необходимо решать задачу поиска дефектов в исполняемом коде программ в соответствии с заданными критериями.

Диссертант рассмотрел множество методов и алгоритмов применяемых для статического анализа программ и предложил свое решение поставленной задачи. Разработал и реализовал межпроцедурный анализ, использующий механизм аннотаций, позволяющий создать краткое описание функции используемое при дальнейшем анализе. Данный механизм обеспечивает как точность анализа (за счет контекстной чувствительности при обработке вызовов), так и масштабируемость (функция анализируется однократно). Разработаны и реализованы внутрипроцедурные алгоритмы – анализ значений, анализ достигающих определений, трансформация удаления мертвого кода. Полученная информация позволяет построить графы

зависимостей программы и графы зависимостей системы, а также используется для поиска дефектов. Разработаны и реализованы алгоритмы поиска пяти типов дефектов – дефекты использования памяти после ее освобождения, двойного освобождения памяти, форматных строк, переполнения буфера и внедрения команд. На основе графов зависимостей программ разработаны и реализованы алгоритмы поиска клонов исполняемого кода, сравнения двух исполняемых файлов, автоматического анализа характера изменений между версиями программ и поиска неисправленных частей в новой версии программ.

Все предложенные диссертантом методы были реализованы в инструменте статического анализа бинарного кода Binside, разрабатываемом в Институте системного программирования им. В.П. Иванникова РАН, и показали необходимую точность и масштабируемость, давая полное решение поставленной задачи. В среднем процент истинных срабатываний находился от 40-60%.

При разработке и реализации методов, описанных в диссертации, Асланян А.К. проделал большой объем работы, в том числе проанализировал и протестировал множество методов и алгоритмов, провел многочисленные эксперименты.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а ее автор, Асланян Айк Каренович, заслуживает присуждения ему ученой степени кандидата физико-математических наук.

Научный руководитель:
с.н.с. ИСП РАН, к.ф.-м.н. Ш. Ф. Курмангалеев
28 декабря 2018 года

Подпись Курмангалеева Ш.Ф. удостоверяю

Директор ИСП РАН,
чл.-корр. РАН, д.ф.-м.н. А.И. Аветисян