Отзыв

официального оппонента
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: в настоящее время проблема повышения качества программного обеспечения промышленного назначения имеет высокую актуальность. Разработчики часто совершают ошибки, которые могут привести к сбоям в работе программы. Повышение безопасности используемого прикладного и системного ПО играет важную роль как в работе больших компаний и организаций, так и для отдельных пользователей. Чем сложнее задача и чем важнее область, в которой используются информационные технологии, тем критичнее становится задача нахождения любых ошибок в программных системах, задействованных в процессах сбора, накопления, обработки, передачи и хранения компьютерных данных.

Существует два основных подхода к анализу программ: статический и динамический. В диссертационной работе использован статический подход, с помощью которого можно анализировать программу без ее реального выполнения. Большинство существующих инструментов статического анализа работают с исходным кодом программы. Однако часто такого анализа недостаточно. Требуется прикладной инструмент статического анализа бинарного кода масштаба в десятки мегабайт.

Структура и содержание диссертации: текст диссертации включает 118 страниц и состоит из введения, четырех глав, заключения, одного приложения и списка литературы, который включает 89 наименований. В тексте имеется 11 рисунков и 22 таблиц.

Во введении обоснована актуальность темы исследования, определены цели и задачи, формулируется их научная новизна и практическая значимость, дано описание структуры и объема диссертационной работы, а также перечислены публикации по теме исследования.

В первой главе приводится обзор существующих методов статического анализа исполняемого кода программ, методов поиска клонов исполняемого кода, сравнения исполняемых файлов и анализа характера изменений программ между версиями. В частности, в разделе 1.3 описаны методы поиска клонов исполняемого кода (семантически близких разделов кода).

Во второй главе описывается общая архитектура разработанного инструментария для статистического анализа исполняемого кода, связанного с поиском дефектов. Предлагаемые методы используют промежуточный язык низкого уровня REIL (Reverse Engineering Intermediate Language), на котором можно эффективно разрабатывать

алгоритмы анализа независимо от платформы. Представлены разработанные автором методы анализа значений, анализа помеченных данных, достигающих определений, трансформация для удаления мертвого кода, анализ динамической памяти. Предлагаемая архитектура разработана с учетом следующих требований: независимость от целевой архитектуры; возможность проведения межпроцедурного, контекстно-чувствительного, чувствительного к потоку данных и к потоку управления анализа; масштабируемость; возможность расширения функционала платформы. Приведенные в таблице 1 результаты тестирования разработанного инструментария показывают его высокую эффективность.

В третьей главе приведен метод сравнения исполняемых файлов и анализа измененных участков кода. Приведена архитектура инструмента поиска клонов кода в исполняемом файле. Разработанный метод отличается высоким уровнем истинных срабатываний, позволяет находить все типы клонов (из рассмотренных трех) и способен анализировать программы размером в десятки мегабайт вне зависимости от целевой архитектуры. Для сравнения исполняемых файлов предложены три алгоритма сопоставления функций. В таблице 2 представлены результаты работы разработанных алгоритмов по поиску клонов, в таблице 3 результаты тестирования инструментария сопоставления функций двух исполняемых файлов, а в таблице 4 результаты работы инструментария анализа характера изменений между версиями программ. Эти результаты подтверждают, что поставленные цели достигнуты.

В четвертой главе описаны методы поиска дефектов. Реализованы детекторы дефектов использования памяти после освобождения, двойного освобождения памяти, форматных строк, переполнения буфера и внедрения команд. Описаны три алгоритма поиска неисправленных частей в новых версиях исполняемых файлов. Как показывают результаты, представленные в таблицах 6-9, разработанный инструментарий показывает более высокий уровень точности, чем другие методы.

В заключении формулируются основные результаты, полученные в ходе диссертационной работы, а также обсуждаются направления дальнейших исследований.

Замечания: Диссертация выполнена на высоком научном уровне. Однако можно отметить отдельные недостатки. В частности, не приводится информация о среднем количестве ошибок второго рода (количестве ненайденных программных ошибок) в отличие от ошибок первого рода, которые приведены в таблицах 10-19. Однако, это замечание не носит принципиального характера и не влияет на общую положительную оценку работы.

Заключение: диссертационная работа Асланяна Айка Кареновича является законченным научным исследованием, выполненным самостоятельно на актуальную тему и на высоком научном уровне. Автореферат диссертации правильно и полно отражает ее содержание. Исследование обладает научно-теоретической и практической значимостью, что подтверждается результатами. Полученные автором результаты достаточно полно отражены в опубликованных статьях, их достоверность подтверждается апробацией на

семинарах и конференциях различного уровня. По теме диссертации опубликовано шесть научных работ, в том числе, три научные статьи опубликованы в рецензируемых журналах, входящих в перечень рекомендованных ВАК РФ, из них одна в журнале, индексируемом в международной базе цитирования Web of Science. Автореферат полно отражает содержание и основные положения диссертации.

Принимая во внимание актуальность темы диссертации, научную новизну и практическую значимость результатов, считаю, что представленная диссертационная работа полностью соответствует всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор, Асланян Айк Каренович, заслуживает присуждения ему ученой степени по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент
доктор физико-математических наук,
старший научный сотрудник,
начальник отдела Курчатовского комплекса НБИКС-природоподобных технологий Национального исследовательского центра «Курчатовский институт» Ильин Вячеслав Анатольевич

25.02.2019

Почтовый адрес: 123182, РФ, Москва, пл. Академика Курчатова, д. 1
Телефон: +7 (499) 196–95–39
Электронная почта: nrcki@nrcki.ru

Подпись сотрудника НИЦ «Курчатовский институт» В.А. Ильина заверяю
Главный ученый секретарь
НИЦ «Курчатовский институт»
доктор физико-математических н

П.А. Форш