ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01
на базе Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Федерального агентства научных организаций РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 15 февраля 2018 года № 2018/04

О присуждении Каушану Вадиму Владимировичу, гражданину РФ ученой степени кандидата технических наук.

Диссертация «Поиск ошибок выхода за границы буфера в бинарном коде программ» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 15 декабря 2017 года, протокол № 2017/26 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Федеральное агентство научных организаций; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Каушан Вадим Владимирович, 1990 года рождения, работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова РАН, ФАНО.

В 2013 году соискатель окончил Московский физико-технический институт (государственный университет).

В 2016 году соискатель окончил аспирантуру Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук, ФАНО.

Научный руководитель – кандидат физико-математических наук Падарян Вартан Андроникович, Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук, отдел «Компиляторных технологий», ведущий научный сотрудник.

Официальные оппоненты:

1. Галатенко Владимир Антонович, доктор физико-математических наук, заведующий сектором Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»,
2. Волконский Владимир Юрьевич, кандидат технических наук, начальник отделения «Системы программирования» Публичного акционерного общества «Институт электронных управляющих машин им. И.С. Брука»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва в своем положительном заключении, подписанном академиком Соколовым И.А., директором ФИЦ ИУ РАН, указала, что диссертационная работа содержит новые научные результаты, имеющие практическую и научную ценность.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертационной работы.

Соискатель имеет 10 опубликованных работ, в том числе по теме диссертации 6 работ, из них 4 — в рецензируемых научных изданиях, в том числе 1 работа — в журнале, индексируемом Web of Science и Scopus.

В работах [1;6] представлен разработанный автором базовый метод символьной интерпретации трасс выполнения. В работах [2;3;5] автором описан метод символьной интерпретации трассы с учётом символьных длин буферов, а также метод поиска ошибок выхода за границы буфера. В рамках работы [4] автором была описана операционная семантика машинных инструкций различных процессорных архитектур для промежуточного представления Pivot, используемого в диссертационной работе.

1. Padaryan VA, Kaushan VV, Fedotov AN. Automated exploit generation for stack buffer overflow vulnerabilities // Programming and Computer Software. — 2015. — Vol. 41, no. 6. — Pp. 373–380.
2. Каушан В. В., Мамонтов А. Ю., Падарян В. А. и др. Метод выявления некоторых типов ошибок работы с памятью в бинарном коде программ // Труды Института системного программирования РАН. — 2015. — Т. 27, № 2. — С. 105–126.
3. Каушан В. В. Поиск ошибок выхода за границы буфера в бинарном коде программ // Труды Института системного программирования РАН. — 2016. — Т. 28, № 5. — С. 135–144.
4. Падарян В. А., Каушан В. В., Гетьман А. И. и др. Методы и программные средства, поддерживающие комбинированный анализ бинарного кода // Труды Института системного программирования РАН. — 2014. — Т. 26, № 1. — С. 251–276.
5. Федотов А. Н., Каушан В. В., Падарян В. А. и др. Поиск некоторых типов ошибок работы с памятью в бинарном коде программ // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — 2015. — С. 103–105.
6. Каушан В. В., Федотов А. Н. Развитие технологии генерации эксплойтов на основе анализа бинарного кода // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — 2015. — С. 77–79.

Диссертационный совет отмечает, что соискателем получены новые научные результаты:

- На основе технологий анализа трасс выполнения программ разработан метод символьного анализа трасс с учётом абстрактной длины переменных-массивов, обрабатываемых в программе. Для анализа не требуется наличие исходных кодов анализируемой программы и отладочной информации. Кроме того, метод позволяет абстрагироваться от используемой архитектуры процессора, а также операционной системы, благодаря чему открываются возможности для анализа широкого круга приложений и платформ, недоступные большинству инструментов динамического анализа.
- На основе метода символьной интерпретации трасс выполнения разработан метод поиска ошибок выхода за границы буфера. Ключевой особенностью метода является способность находить ошибки, которые не проявились во время запуска анализируемой программы.

Разработанные методы были реализованы в виде программного инструмента.

Полученные и представленные результаты отвечают специальности 05.13.11, поскольку относятся к области исследований «Модели, методы и алгоритмы проектирования и анализа программ и программных систем, их эквивалентных преобразований, верификации и тестирования».

Теоретическая значимость исследования состоит в том, что:

- применительно к проблеме поиска ошибок по трассам выполнения использован аппарат символьных вычислений;
- применительно к анализу операций работы со строками продемонстрирована возможность абстрагирования от длин обрабатываемых строк.

Значение полученных соискателем результатов исследования для практики состоит в том, что:

- разработанный программный инструмент позволяет искать ошибки в программах, работающих на процессорных архитектурах, отличных от

x86/x86_64 при наличии описания операционной семантики машинных инструкций целевой архитектуры;

- разработанные методы могут использоваться для развития других существующих инструментов поиска ошибок.

Достоверность результатов исследования заключается в том, что:

- метод позволил обнаружить все ошибки на тестовом наборе, состоящем из программ с известными ошибками выхода за границы буфера;
- полученные экспериментальные данные соответствуют теоретическим результатам.

Личный вклад соискателя состоит в разработке метода символьной интерпретации с использованием абстрактной длины буферов, разработке метода поиска ошибок выхода за границы буфера на основе метода символьной интерпретации, реализации программного инструмента на основе предложенных методов, апробации методов, подготовке основных публикаций по выполненной работе.

На заседании 15 февраля 2018 года диссертационный совет принял решение присудить Каушану В.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 15 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 15, против – 0, недействительных бюллетеней – 0.

Председатель диссертационного совета,
член-корр. РАН Аветисян А. И.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

15 февраля 2018 года