ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного на базе
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Министерства науки и высшего образования РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 19 октября 2023 года № 2023/12

О присуждении Куцу Даниилу Олеговичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Метод моделирования косвенной адресации в рамках динамической символьной интерпретации»я по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 17 августа 2023 года, протокол № 2023/05 диссертационным советом 24.1.120.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; 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 Куц Даниил Олегович, 1994 года рождения.

В 2018 году соискатель окончил факультет информатики и систем управления Московского государственного технического университета имени Н. Э. Баумана по специальности «Противодействие техническим разведкам». В 2022 году соискатель окончил аспирантуру в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Работает стажером-исследователем в лаборатории системного программирования и информационной безопасности ФГБУН Института системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Диссертация выполнена в лаборатории системного программирования и информационной безопасности ФГБУН Института системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – кандидат технических наук Федотов Андрей Николаевич, старший научный сотрудник отдела компиляторных технологий ФГБУН Института системного программирования им. В. П. Иванникова РАН.

Официальные оппоненты:

1. Шабанов Борис Михайлович, член-корреспондент РАН, доктор технических наук, доцент, директор Межведомственного Суперкомпьютерного Центра РАН, заместитель директора по научной работе Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»,
2. Дмитрий Олегович Маркин, кандидат технических наук, сотрудник ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное учреждение "Федеральный исследовательский центр Институт прикладной математики им. М.В. Келдыша Российской академии наук", г. Москва в своем положительном заключении, подписанном старшим научным сотрудником отдела инструментального и прикладного программного обеспечения ИПМ им. М.В. Келдыша РАН кандидатом физико-математических наук Юрием Андреевичем Климовым, указала, что диссертация является законченной научно-

квалификационной работой, в которой решена актуальная задача разработки нового метода моделирования косвенной адресации в контексте динамической символьной интерпретации, и полностью соответствует паспорту научной специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Соискатель имеет 9 опубликованных работ, в том числе по теме диссертации опубликовано 4 работы, из них в рецензируемых научных изданиях опубликовано 4 работы.

Публикации посвящены разработке методов моделирования косвенных переходов в бинарном коде, разработке методов моделирования чтений по символьному адресу в рамках динамической символьной интерпретации, исследованию производительности SMT-решателей применяемых в динамическом анализе программ. Вклад соискателя в совместных публикациях заключается в реализации подсистемы генерации данных в составе инструмента динамической символьной интерпретации Anxiety, в описании применения SMT-решателей и подготовке набора данных для проведения экспериментов, в разработке метода поиска и моделирования косвенных переходов, обработке и интерпретации экспериментальных результатов, подготовке статей.

Наиболее значимые работы по теме диссертации:

1. Kuts, D. Towards symbolic pointers reasoning in dynamic symbolic execution [Text] / D. Kuts // 2021 Ivannikov Memorial Workshop (IVMEM). — IEEE, 2021. — P. 42—49. — (Scopus, WoS)
2. Sydr: Cutting Edge Dynamic Symbolic Execution / A. Vishnyakov [et al.] // 2020 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE, 2020. — P. 46—54. — (Scopus, WoS).
3. SMT Solvers in Application to Static and Dynamic Symbolic Execution: A Case Study [Text] / N. Malyshev [et al.] // 2019 Ivannikov Ispras Open Conference (ISPRAS). — IEEE, 2019. — P. 9—15. — (Scopus, WoS).

4. Anxiety: a dynamic symbolic execution framework [Text] / A. Gerasimov [et al.] // 2017 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE, 2017. — P. 16—21. — (Scopus, WoS)

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 диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- Разработан метод поиска и моделирования косвенных переходов в рамках динамической символьной интерпретации. Предложены алгоритмы обнаружения косвенных переходов в бинарном коде и определения границ таблицы переходов в памяти программы. Проведена экспериментальная оценка эффективности алгоритма, которая показала увеличение числа символьных ветвей и открытие новых путей исполнения в анализируемых программах.
- Разработан метод моделирования чтений памяти по символьно вычисляемому адресу. Метод моделирует символьные чтения с помощью выражения, представляющее собой двоичное дерево поиска. Эффективность выбранного способа построения ограничений была продемонстрирована. Экспериментальная оценка метода при проведении анализа программ показала существенный прирост новых неисследованных ранее условных переходов и увеличение тестового покрытия на этих программах.
- Предложенные методы были реализованы в программных системах, которые используются в Центре доверенного искусственного интеллекта ИСП РАН и ООО «Код Безопасности».

Теоретическая значимость исследования обоснована тем, что:

- разработаны метод поиска и моделирования косвенных переходов и метод моделирования чтений памяти по символьно вычисляемому адресу, которые применимы при анализе больших программных систем;

- изучены различные способы построения ограничений для моделирования чтений памяти по символьно вычисляемому адресу. Проведена экспериментальная оценка эффективности этих способов с использованием различных SMT-решателей.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- разработанные методы позволяют улучшать результаты динамического анализа и приводить к обнаружению новых программных дефектов;
- разработанные методы используются в Центре доверенного искусственного интеллекта ИСП РАН;
- разработанные методы внедрены и используются ООО «Код Безопасности» в рамках следования безопасному циклу разработки ПО.

Оценка достоверности результатов исследования выявила:

- разработанные методы, реализованные в составе инструмента динамической символьной интерпретации Sydr, показывают свою применимость в рамках динамического анализа программ, гибридного фаззинга;
- экспериментально показана эффективность предложенных методов при проведении динамического анализа бинарных программ.

Личный вклад соискателя состоит в разработке метода поиска и моделирования косвенных переходов, метода моделирования чтений памяти по символьно вычисляемому адресу, реализации методов, обработке и интерпретации экспериментальных результатов, подготовке статей.

В ходе защиты диссертации были высказаны следующие критические замечания:

- отсутствие экспериментального сопоставления с существующими инструментами, приведенными в обзоре работ;
- не приведено формальное описание некоторых разработанных алгоритмов;

- ограничение применимости разработанных методов аппаратными платформами с архитектурой x86_64, нет пояснения по работоспособности методов для иных процессорных архитектур (RISC-V, PowerPC, ELBRUS);
- зависимость реализации разработанного метода от частных параметров, которые влияют на точность и производительность системы;
- при экспериментальной оценке методов не учитывалось обнаружение ошибок.

Соискатель Куц Даниил Олегович согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 19 октября 2023 г. диссертационный совет принял решение присудить Куцу Даниилу Олеговичу ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 22 человек, входящих в состав совета, проголосовали: за – 16, против – 0.

Заместитель председателядиссертационного совета,
доктор физико-математических наук Петренко А. К.

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

19 октября 2023 года