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 13 июня 2024 года № 2024/09

О присуждении Шимчику Никите Владимировичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Исследование и разработка методов поиска уязвимостей в программах на C и C++ на основе статического анализа помеченных данных» по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 12 апреля 2024, протокол № 2024/06 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 Шимчик Никита Владимирович, 1994 года рождения.

В 2017 году соискатель окончил факультет вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова. В 2021 году соискатель окончил аспирантуру Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – кандидат физико-математических наук Игнатьев Валерий Николаевич, старший научный сотрудник отдела компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

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. Маркин Дмитрий Олегович, кандидат технических наук, сотрудник Федерального государственного казённого военного образовательного учреждения высшего образования «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 заведующим Информационно-

издательским отделом ИПМ им. М.В. Келдыша РАН, доктором физико-математических наук Михаилом Михайловичем Горбуновым-Посадовым, указала, что диссертационная работа является законченным научным исследованием по актуальной тематике статического анализа для поиска уязвимостей в программах и соответствует требованиям ВАК РФ, предъявляемым к работам на соискание степени кандидата технических наук по специальности 2.3.5 — «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Соискатель имеет 8 опубликованных работ, в том числе по теме диссертации опубликовано 8 работ, из них в рецензируемых научных изданиях опубликовано 4 работы.

Публикации посвящены поиску уязвимостей в программах на основе статического анализа помеченных данных. Вклад соискателя заключается в реализации анализа помеченных данных на основе символьного выполнения в инструменте SharpChecker, а также разработке и реализации инструмента Irbis и предлагаемых методов и алгоритмов повышения точности, полноты и масштабируемости проводимого им анализа.

Наиболее значимые работы по теме диссертации:

1. Шимчик, Н. Поиск уязвимостей при помощи статического анализа помеченных данных. / Н. Шимчик, В. Игнатьев // Труды Института системного программирования РАН. — 2019. — Т. 31, № 3. — С. 177—190.

2. Comparative analysis of two approaches to static taint analysis / M. Belyaev, N. Shimchik, V. Ignatyev, A. Belevantsev // Programming and Computer Software. — 2018. — Т. 44, № 6. — pp. 459—466.

3. Шимчик, Н. Irbis: статический анализатор помеченных данных для поиска уязвимостей в программах на C/C++ / Н. Шимчик, В. Игнатьев, А. Белеванцев // Труды Института системного программирования РАН. — 2023. — Т. 34, № 6. — С. 51—66.

4. Shimchik, N. Improving Accuracy and Completeness of Source Code Static Taint Analysis / N. Shimchik, V. Ignatyev, A. Belevantsev // 2021 Ivannikov Ispras Open Conference (ISPRAS). — IEEE. 2021. — С. 61—68.

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 алгоритм направленного распространения пометок в статическом анализе помеченных данных, позволяющий уменьшить количество выполняемых итераций алгоритма IFDS для помеченных глобальных переменных. Была доказана корректность данного алгоритма и проведена экспериментальная оценка его влияния на масштабируемость анализа. Оценка показала ускорение анализа, которое в зависимости от анализируемого проекта может достигать 55%, а также уменьшение потребления оперативной памяти до 11%.
- Разработан алгоритм снятия пометок с тех целочисленных переменных, для которых в коде программы в явном виде проверяется верхняя и нижняя границы их возможных значений. Этот алгоритм повышает точность анализа за счёт устранения ложных срабатываний, вызванных использованием данных, полученных извне, для которых в явном виде выполняется проверка допустимости диапазона их значений. Экспериментальная проверка показала повышение точности анализа без потери истинных срабатываний, а на тестовом наборе Juliet применение данного алгоритма позволило достичь 100% точности на выбранном наборе типов уязвимостей.
- Разработан алгоритм анализа косвенных вызовов на основе межпроцедурного анализа потоков данных задачи IFDS. Данный алгоритм позволяет находить кандидатов для вызова по указателю, что повышает полноту анализа за счёт возможности исследования межпроцедурных путей, проходящих через такие вызовы. Экспериментальное сравнение показало, что данный алгоритм смог найти хотя бы одного кандидата как минимум в

30% вызовов, по сравнению с анализом на основе типов функций, и в отличие от него не подставляет заведомо ложных кандидатов.

- Разработан метод проверки консистентности путей распространения пометок, обнаруженных во время анализа. Данный метод позволяет выбирать из множества путей между вершинами графа распространения помеченности те, которые не являются неконсистентными по выбранным критериям. Предложены три критерия консистентности пути для косвенных вызовов, виртуальных вызовов, а также в вызовов с множественными кандидатами в полнопроектном анализе.
- Предложенные методы и алгоритмы были реализованы в инструменте для поиска уязвимостей Irbis, который входит в состав статического анализатора Svace и используется в ООО "БАЗИС" и ООО НТЦ "Фобос-НТ".

Теоретическая значимость исследования обоснована тем, что:

- разработаны методы и алгоритмы, предназначенные для повышения точности, полноты и масштабируемости статического анализа помеченных данных и применимые для анализа реальных проектов;
- для алгоритма направленного распространения помеченности была приведена теоретическая оценка влияния пометок на глобальных переменных на общее время анализа, по сравнению с пометками на локальных значениях и формальных аргументах функций, а также доказана корректность алгоритма.

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

- предложенные методы и алгоритмы позволяют находить больше потенциальных уязвимостей, уменьшить количество ложных срабатываний, а также повысить масштабируемость анализа;
- реализованный на основе этих методов и алгоритмов инструмент Irbis пригоден для анализа проектов в миллионы строк кода и способен обнаруживать такие реальные уязвимости как Heartbleed;

- инструмент был внедрён и используется в ООО "БАЗИС" и ООО НТЦ "Фобос-НТ", что подтверждается предоставленными актами о внедрении (Акт о внедрении ООО "БАЗИС" от 20.05.2024 г., Акт о внедрении ООО НТЦ "Фобос-НТ" от 27.05.2024 г.).

Оценка достоверности результатов исследования выявила:

- разработанные методы и алгоритмы, реализованные в составе инструмента статического анализа помеченных данных Irbis, показывают свою применимость в рамках статического анализа программ для поиска уязвимостей;
- экспериментально показана эффективность предложенных методов при анализе реальных проектов и Juliet Test Suite for C/C++;
- проведено экспериментальное сравнение с несколькими реализациями анализа помеченных данных в других инструментах статического анализа программ.

Личный вклад соискателя состоит в разработке алгоритма анализа косвенных вызовов на основе IFDS, алгоритма снятия пометок с целочисленных переменных, алгоритма направленного распространения пометок, метода проверки консистентности путей, их реализации в инструменте Irbis, обработке и интерпретации экспериментальных результатов, подготовке публикаций.

В ходе защиты диссертации были высказаны следующие критические замечания:

- отсутствие обоснования корректности и оценки сложности алгоритмов анализа косвенных вызовов и снятия помеченности;
- отсутствует таблица, демонстрирующая эффект от применения совокупности предложенных алгоритмов;
- использование анализа косвенных вызовов с ограничениями по времени и глубине не гарантирует полноту анализа;
- предложенная эвристика для обнаружения новых истоков работает на ограниченном множестве функций;

- в большинстве таблиц, отражающих результаты применения отдельных методов и алгоритмов, оценка результатов анализа происходит только на проектах Juliet Test Suite и OpenSSL.
- недостаточно формальное описание некоторых разработанных алгоритмов;
- не приведена мотивация для выбора типов поддерживаемых в инструменте уязвимостей.

Соискатель Шимчик Никита Владимирович согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 13 июня 2024 г. диссертационный совет принял решение присудить Шимчику Никите Владимировичу 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 21 человек, входящих в состав совета, проголосовали: за – 15, против – 0.

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

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

13 июня 2024 г.