УТВЕРЖДАЮ
Директор Федерального государственного
учреждения «Федеральный
ельский центр «Информатика и
» Российской академии
АН),

И.А. Соколов
« 15» 04 2019 г.

ОТЗЫВ

ведущей организации ФИЦ ИУ РАН на диссертацию Дудиной Ирины Александровны «Поиск ошибок переполнения буфера в исходном коде программ с помощью символьного выполнения», представленную к защите на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Статический анализ исходного кода является одним из общепризнанных методов обнаружения ошибок в программах на стадии разработки. В частности, он применяется для поиска ошибок переполнения буфера, которые, не будучи вовремя обнаруженными и устранёнными, часто становятся причиной появления эксплуатируемых уязвимостей. Существует множество различных методов поиска ошибок в рамках подхода статического анализа, каждый из которых в силу алгоритмической неразрешимости этой задачи реализует некоторый компромисс между масштабируемостью анализа, количеством найденных ошибок и процентом ложных срабатываний. Однако инструменты, реализующие алгоритмы промышленного статического анализа, удовлетворяющие современным требованиям (анализ программ из миллионов строк кода, умеренное количество ложных срабатываний, чувствительность к путям и контексту), являются закрытыми. Таким образом, **актуальной** представляется задача построения детектора переполнения буфера, удовлетворяющего этим требованиям.

В диссертации получены следующие результаты, обладающие **научной новизной**:

1. Критерий ошибочной ситуации, приводящей к переполнению буфера, использующийся для анализа функции как точки входа в программу с учётом возможных неизвестных предусловий функции.
2. Различающий пути выполнения алгоритм межпроцедурного анализа для обнаружения переполнения буфера константного размера, основанный на символьном выполнении с объединением состояний и методе резюме.
3. Алгоритм анализа для поиска переполнения буфера произвольного размера.
4. Основанные на предложенных алгоритмах методы поиска переполнения при работе со строками и данными из недоверенного источника.

Достоверность результатов исследования обеспечивается обоснованностью математических рассуждений и доказательств, успешной программной реализацией предложенных подходов в инструменте статического анализа, апробацией полученных результатов на конференциях различного уровня.

Теоретическую значимость представляют методы поиска переполнения буфера с помощью символьного выполнения, для которых показана корректность построенных достаточных условий ошибки. Построенные методы применимы к буферам как константного, так и произвольного размера, а также учитывают специфику буферов-строк и буферов с недоверенными данными.

Практическая значимость работы заключается в реализации этих методов в статическом анализаторе Svace, внедрённом в том числе в компании Samsung и некоторых российских компаниях.

Общая характеристика работы. Диссертация состоит из введения, семи глав, заключения, списка литературы из 76 источников и одного приложения, изложена на 145 страницах.

Во введении обосновывается актуальность работы, формулируются цель и задачи исследования, приводятся его результаты и сведения об апробации.

Первая глава посвящена обзору существующих методов и инструментов обнаружения переполнения буфера, исследованию популярных тестовых наборов и уязвимостей из реальных проектов для определения требований к разрабатываемому подходу.

Во второй главе рассматриваются особенности проведения анализа в отсутствие информации о предусловиях функции; с учётом этих особенностей предлагается критерий ошибочной ситуации, использующийся в дальнейшем при построении алгоритмов анализа.

В третьей главе описывается основной алгоритм внутрипроцедурного анализа для обнаружения переполнения буфера константного размера. Алгоритм основывается на подходе символьного выполнения с объединением состояний, благодаря чему обеспечивается чувствительность к путям. Предложен метод построения достаточных условий ошибки, использующий разработанный критерий ошибочной ситуации, для него доказана теорема о корректности получаемых условий.

В четвёртой главе предлагается алгоритм межпроцедурного анализа для поиска переполнения буфера с константным размером. Он основан на методе резюме и заключается в том, что результаты внутрипроцедурного анализа некоторой функции используются при анализе инструкции вызова этой функции, при этом каждая функция анализируется один раз. Описывается ряд расширений внутрипроцедурного алгоритма, позволяющих проводить более полный межпроцедурный анализ.

В пятой главе рассматриваются методы обнаружения переполнения буфера при работе со строками и данными из недоверенного источника, основанные на предложенных ранее подходах.

В шестой главе предлагаются два метода поиска переполнения буфера произвольного размера: первый использует построенный в главах 2–5 формализм для оценки возможного размера буфера, а второй непосредственно применяет сформулированный во второй главе критерий ошибки, что требует работы с кванторами всеобщности в проверяемых на совместность логических

формулах.

В седьмой главе описаны детали реализации предложенных алгоритмов в статическом анализаторе Svace. Разработанные детекторы протестированы на коде операционных систем Android и Tizen, результаты экспериментов подтверждают приемлемое количество ложных срабатываний. Покрытие ошибочных ситуаций оценивалось с помощью тестового пакета Juliet Test Suite. Сравнение по покрытию со статическим анализатором Infer оказалось в пользу инструмента Svace.

В заключении приводятся основные результаты работы.

Замечания по работе. По диссертации могут быть сделаны отдельные замечания:

1. В разделе 4.3.1 рассматривается применение межпроцедурного алгоритма для анализа вызовов библиотечных функций с помощью их спецификаций, но не приводится перечень или описание множества функций, для которых требуется спецификация.

2. В разделе 7.2.1, посвящённом особенностям реализации детекторов, упоминаются, но подробно не описываются методы упрощения получаемых формул и быстрой проверки формулы на несовместность с помощью интервалов значений.

Заключение. Перечисленные замечания не влияют на общую положительную оценку диссертационной работы и не снижают значимость полученных теоретических и практических результатов. Диссертация в соответствии с требованиями «Постановления Правительства Российской Федерации о порядке присуждения учёных степеней» от 24.09.2013 г. №842 является законченной научно-квалификационной работой, в которой предложены новые методы и средства решения актуальной научной задачи – поиска ошибок переполнений буфера. Диссертация полностью соответствует паспорту специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей. По теме диссертации автором опубликовано 8 работ. Автореферат правильно

отражает содержание диссертации и её основные результаты.

Автор диссертации, Дудина Ирина Александровна, заслуживает присуждения учёной степени кандидата физико-математических наук по указанной специальности.

Отзыв обсуждён и утверждён на заседании секции Учёного совета ИПИ РАН Федерального исследовательского центра «Информатика и управление» Российской академии наук, протокол № 3 от 11.04.2019 г.

Руководитель Отделением №6,
доктор физ-мат. наук В.И. Синицин
«12» 04 2019 г.

Старший научный сотрудник
отдела 61, кандидат тех. наук В.В. Белоусов
«12» 04 2019 г.