ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Шимчика Никиты Владимировича
«Исследование и разработка методов поиска уязвимостей в программах на C и C++ на основе статического анализа помеченных данных»,
представленную на соискание ученой степени
кандидата технических наук по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Шимчик Н.В. занимается исследованиями в области статического анализа исходного кода программ. Целью его диссертационной работы является разработка методов и алгоритмов поиска уязвимостей и ошибок в исходном коде с помощью статического анализа помеченных данных. Основными требованиями к предлагаемым методам являются обеспечение минимального количества пропущенных ошибок и высокая масштабируемость, позволяющая анализировать проекты из нескольких миллионов строк кода. Второстепенным, но важным требованием является приемлемая для практического применения доля истинных предупреждений (не менее половины).

Тема диссертационной работы актуальна, т. к. разработка методов, удовлетворяющих перечисленным требованиям, и их реализация в статическом анализаторе позволит повысить надежность программ и безопасность данных за счет раннего обнаружения ошибок, связанных с помеченными данными. Такие ошибки являются причиной уязвимостей, которые могут привести как к утечке конфиденциальных данных, так и, наоборот, предоставить злоумышленнику возможность внедрения данных или кода.

Н.В. Шимчик разработал набор алгоритмов для повышения полноты, точности и масштабируемости анализа помеченных данных, реализация которых позволила создать полезный для практического применения инструмент статического анализа кода на Си и C++. Разработанный алгоритм анализа косвенных вызовов на основе задачи IFDS, которая применяется в анализе помеченных данных, в совокупности с предложенными эвристиками автоматического обнаружения истоков повышает полноту результатов. Для повышения точности автором предложены алгоритмы двухэтапного анализа, выполняющего консервативную фильтрацию результатов нечувствительного к путям выполнения анализа помеченных данных, а именно, проверку консистентности путей выполнения, а также снятие помеченности с целочисленных переменных. Вместе предложенные алгоритмы на 25% сократили количество ложных предупреждений. Предложенный алгоритм направленного распространения констант ускорил анализ набора тестов Juliet Test Suite в 2

раза, а на других проектах обеспечил возможности для анализа большего количества потенциальных путей распространения помеченных данных за то же время.

Одним из наиболее значимых результатов работы является разработка и реализация такого набора алгоритмов, который позволил из «движка» распространения помеченных данных получить инструмент, удовлетворяющий принятым в индустрии показателям точности и масштабируемости и позволяющий находить реальные ошибки в коде, как, например, причину известной уязвимости Heartbleed в библиотеке OpenSSL. Среди аналогичных инструментов существуют либо «движки» без детекторов ошибок (Phasar), либо специализированные инструменты для других языков (FlowDroid), либо анализаторы, непригодные для проверки реальных проектов.

Практическая значимость работы заключается в реализации всех предложенных методов в инструменте статического анализа помеченных данных Irbis на основе компиляторной инфраструктуры LLVM. Анализатор интегрирован в разрабатываемый в ИСП РАН инструмент Svace.

Хочется отметить высокую продуктивность диссертанта, который, помимо работы над Irbis, вовлечен и в другие проекты, связанные с применением машинного обучения для поиска ошибок в коде. Диссертант успешно руководит студентами магистратуры и бакалавриата ВМК МГУ, участвует в реализации поточного курса «Формальные языки и автоматы» на ВМК МГУ и ФКН ВШЭ, ведет семинарские занятия, составляет и проверяет задачи контрольных и практических работ.

Считаю, что диссертационная работа Н.В. Шимчика соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата технических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а ее автор, Никита Владимирович Шимчик, заслуживает присуждения ему ученой степени кандидата технических наук.

Научный руководитель,
с.н.с. ИСП РАН, к.ф.-м.н. Игнатьев В.Н.
11 апреля 2024 года

Подпись Игнатьева В.Н. удостов
Ученый секретарь ИСП РАН, к.т Самоваров О.И.