ОТЗЫВ

научного руководителя на диссертацию Каушана Вадима Владимировича "Поиск ошибок выхода за границы буфера в бинарном коде программ", представленную на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Ошибки работы с памятью способны катастрофически ухудшить безопасность ПО. Висячие указатели или выход за пределы массива в лучшем случае незамедлительно приводят к аварийному завершению, в худшем – нарушают целостность программы, что в свою очередь вызывает каскадное нарастание ошибок произвольной природы. Несмотря на многолетние попытки принципиально избавиться от ошибок работы с памятью, их доля в общей статистике эксплуатируемых ошибок стабильно держится выше 10%, а разработка ПО на небезопасных языках, таких как Си/Си++, активно продолжается. При наличии исходного кода можно применять инструменты статического анализа, хорошо себя зарекомендовавшие на практике. Но в условиях отсутствия исходных кодов и отладочной информации, что является характерной ситуацией для проприетарного ПО, приходится искать ошибки, располагая только исполняемым кодом. Решению этой актуальной задачи посвящена диссертация В.В. Каушана, а именно: разработке методов, позволяющих находить ошибки выхода за границы буфера в бинарном коде программ.

Свою научную деятельность в ИСП РАН В.В. Каушан начал еще студентом 3-го курса ФУПМ МФТИ, инициативно подключившись к работе одной из команд отдела компиляторных технологий ИСП РАН. В.В. Каушан выделялся среди всех остальных студентов неподдельным интересом к исследованиям в области анализа программ, а уже имеющиеся развитые навыки в области обратной инженерии бинарного кода и целеустремленность, позволяли ему успешно решать сложные задачи в кратчайшие сроки.

Накопленные за время учебы знания позволили В.В. Каушану при работе над диссертацией поставить перед собой сложную задачу, требующую компетенций в различных областях: компиляторных технологиях, компьютерной безопасности, операционных системах, технологиях разработки ПО.

Недостатки и ограничения существующих походов к поиску ошибок в бинарном коде потребовали разработки новых методов, применимых к пользовательскому и системному коду, работающих вне зависимости от модели процессора, для которого был построен исполняемый код.

Работая над диссертацией, Каушан В.В. последовательно и самостоятельно решал поставленные задачи. Им был разработан автоматизированный метод поиска ошибок

выхода за границы буфера на основе символьной интерпретации трассы. Метод позволяет находить ошибки, даже если они не проявлялись в виде аварийного завершения программы в анализируемой трассе. В ходе символьной интерпретации моделируются произвольные длины переменных-массивов и оценивается влияние этих длин на безопасность выполнения программы. Вся необходимая высокоуровневая информация о программе, такая как организация циклов и размещение переменных, восстанавливается в результате обратной инженерии исполняемого кода. Каушаном В.В. были разработаны вспомогательные методы, улучшающие поиск ошибок: посредством расширения покрытия кода трассами и за счет выявления встроенных вызовов библиотечных функций, что характерно для кода, полученного современными оптимизирующими компиляторами. Разработанные методы были реализованы, их работоспособность была показана на примерах, работающих под управлением различных операционных систем: Windows, Linux, VxWorks. Полученные диссертантом результаты были опубликованы в авторитетных изданиях, докладывались и обсуждались на конференциях.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей – а ее автор, Каушан Вадим Владимирович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.11.

Научный руководитель: в.н.с. ИСП РАН, к.ф.-м.н. В.А. Падарян
29 ноября 2017 года

Подпись Падаряна В.А. удостоверяю

директор ИСП РАН Аветисян А.И.