

ОТЗЫВ

научного руководителя на диссертацию Чан Ти Тхиена
«Разработка нового метода автоматизированного тестирования программных библиотек», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Современное программное обеспечение, как правило, в значительной мере использует программные компоненты с открытым исходным кодом, в частности – программные библиотеки. Число сторонних компонентов, задействуемых при разработке программ, среди прочего зависит от их типа и среды функционирования и может составлять несколько сотен. При этом популярные проекты с открытым исходным кодом постоянно развиваются: расширяются их функциональные возможности, выполняется рефакторинг исходного кода. Следствием этого является возникновение ошибок в исходном коде программных библиотек.

Актуальность задачи автоматизированного динамического тестирования программных библиотек с целью поиска в них ошибок обуславливается отсутствием методов формального доказательства отсутствия ошибок в сколь бы то ни было значимой реальной кодовой базе. Методы статического анализа применимы к большим кодовым базам, однако допускают ложные срабатывания и могут пропускать ошибки. Поэтому актуальной является разработка методов динамического рандомизированного (фаззинг-) тестирования, при должной реализации почти не допускающих ложных срабатываний и являющимся необходимым дополнением к методам статического анализа. В случае программных библиотек в связи с их быстрым изменением и большим разнообразием используемых сред сборки важно обеспечить как можно большую автоматизацию запуска фаззинга для данной библиотеки.

В результате проведенных исследований соискатель предложил следующие методы:

- метод определения составляющих программный интерфейс библиотеки экспортируемых функций (API) и передачи однопоточного буфера данных фаззера для аргументов тестируемой функции в фаззинг-обертке;
- метод автоматической генераций фаззинг-оберток для экспортируемых функций программных библиотек, написанных на языках программирования Си и Си++, в условиях отсутствия контекста использования и с учетом контекста использования.

Разработанные методы позволяют существенно автоматизировать труд эксперта-аналитика по созданию фаззинг-оберток, что в свою очередь позволяет подвергать фаззинг-тестированию значительно больший объем кодовой базы в единицу времени.

Разработанный программный продукт был использован в работе испытательной лаборатории ООО НТЦ «Фобос-НТ» для автоматизации создания фаззинг-оберток при выполнении фаззинг-тестирования исследуемого программного обеспечения интерпретаторов Python, PHP, Lua (в отношении исходных кодов указанных интерпретаторов, написанных на языках программирования Си и Си++), выполнявшегося в интересах клиентов испытательной лаборатории в ходе сертификационных испытаний в системе сертификации ФСТЭК России.

Разработанный программный продукт используется для развития технологических возможностей разрабатываемой в ИСП РАН системы определения поверхности атаки Natch с целью автоматизации генерации оберток для функций, обрабатывающих данные, поступающие от пользователей анализируемых программных систем.

Диссертационная работа Чан Ти Тхиена содержит как научную новизну, так и большую практическую значимость. Результаты, полученные в диссертации, доказывались соискателем на международных и российских конференциях. По теме диссертации опубликовано 5 работ, в том числе 2 статьи в научных изданиях, индексируемых системами Scopus и Web of Science, одно свидетельство о государственной регистрации программ для ЭВМ.

Соискатель проявил себя как ответственный, исполнительный и способный исследователь, умеющий ставить и решать актуальные задачи в области технических наук.

Следует отметить, что соискатель обладает опытом научного руководства у студентов бакалавриата, принимал участие в оценке результатов самостоятельных работ, участвовал в подготовке комплектов обучающих материалов для студентов бакалавриата.

Диссертационная работа Чан Ти Тхиена, представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, удовлетворяющей всем требованиям, предъявляемым к кандидатским диссертациям. Считаю, что ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Научный руководитель
Академик РАН,
доктор физико-математических наук

15.06.2023

Аветисян Арутюн Ишханович