УДК 004.056

ОЦЕНКА ЭФФЕКТИВНОСТИ МУТАТОРА ВСТРОЕННОГО ФАЗЗЕРА В ЯЗЫКЕ ПРОГРАММИРОВАНИЯ GOLANG

Барышев Д.А. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Юганссон А.Н.
(Университет ИТМО)

Фаззеры являются одним из самых универсальных инструментов предназначенных для поиска багов в программном обеспечении. Процесс поиска багов полагается на запуск программного обеспечения с различными входными данными, которые генерируются мутатором. В данной работе рассматривается мутатор встроенного фаззера в языке Golang. Были запущены тестовые версии фаззера с модифицированным исходным кодом. Для каждого мутатора была проведена оценка его эффективности, и по полученным результатам были составлены рекомендации по повышению эффективности мутатора для фаззинга в языке Golang.

Введение. Эффективность фаззера определяется количеством найденных им аварийных завершений в программном обеспечении. Поиск аварийных завершений осуществляется с помощью запуска программы со случайными входными данными, которые были итеративно получены вследствие мутаций сидов – исходных данных, составленных самим разработчиком. Задачу мутации над входными данными совершает мутатор, от него зависит как обнаружение новых аварийных завершений, так и получение нового покрытия кода, для расширения области обнаружения аварийных завершений. Следовательно эффективность фаззера прямо коррелирует с эффективностью мутатора. Предметом исследования является мутатор фаззера, включенного в стандартную библиотеку языка Golang.

Основная часть. Встроенный фаззер в языке golang способен проводить мутации над основными типами данных, такими как int, float, []byte и string. Более простые типы, int и float, имеют до четырех мутаций, например, добавление другого значения к исходному или умножение на него. В свою очередь, байтовые и обычные строки на данный момент имеют 18 различных мутаций. Разработаны критерии оценки эффективности мутаций и выбраны программы, на которых будут проводиться тестовые запуски. Для тестирования каждой программы была собрана отдельная версия фаззера с изменённым исходным кодом, включающим единственную мутацию.

Выводы. Проведена оценка эффективности мутатора для фаззинга байтовых строк в языке Golang. Даны рекомендации по повышению эффективности мутатора для фаззинга в языке Golang.

Барышев Д.А. (автор) Подпись

Юганссон А.Н. (научный руководитель) Подпись