УДК 004.415.53

ПРИМЕНЕНИЕ АТРИБУТНЫХ ГРАММАТИК В СИСТЕМАХ ГЕНЕРАЦИИ ТЕСТОВ

Садырин Д.С.
Университет ИТМО, Санкт-Петербург
Научный руководитель – к.т.н., доцент Дергачев А.М.
Университет ИТМО, Санкт-Петербург

Исследуется проблема генерации программ-тестов с заданной статической семантикой на языке программирования высокого уровня PHP.

Введение. Рассматривается подход для генерации тестов для компилятора с использованием атрибутных грамматик.

Основная часть.
В ходе выполнения диссертационной работы был написан транслятор с языка программирования высокого уровня PHP в представление для графовой базы данных, для последующего поиска уязвимости Object Injection. Возникла необходимость тестирования написанного транслятора.
Для этого необходимо производить генерацию примеров на языке программирования, как синтаксически корректных, так и семантически, то есть подходящих под некоторые заданные ограничения. Например, определенное количество классов, методов, условных операторов или переменных в программе.
Статическая семантика дополняет описание синтаксиса языка, сужая класс допустимых программ. Необходимо сгенерировать примеры, удовлетворяющие всем правилам статической семантики. Для генерации необходимо задать формальное описание грамматики языка и формальное описание контекстных ограничений. Для описания контекстных ограничений исходного языка используются атрибутные грамматики. Требования контекстных условий необходимо трансформировать в явные зависимости между отдельными конструкциями языка (между атрибутами при нетерминалах атрибутной грамматики). Необходимо построить систему отношений между атрибутами нетерминалов в синтаксическом дереве разбора такую, что этому дереву разбора будет соответствовать семантически корректная программа.
Во время генерации примеров производится также генерация эксплойта для Object Injection, далее производится трансляция кода примера, с помощью графовой базы данных строится эксплойт и сравнивается с построенным на этапе генерации. Несоответствие построенного эксплойта сгенерированному ранее является признаком наличия ошибки в коде транслятора.

Выводы. Предложенный подход применен для тестирования транслятора языка программирования PHP.

Садырин Д.С. (автор)

Дергачев А.М. (научный руководитель)