РЕЦЕНЗИЯ

на выпускную квалификационную работу студента 4 курса кафедры информационно-аналитических систем СПбГУ Батоева Константина Алановича, обучающегося по направлению 010500 (02.03.03) (математическое обеспечение и администрирование информационных систем)

Тема выпускной квалификационной работы:
Композициональное символьное исполнение CIL-кода

Целью выпускной квалификационной работы является реализация символьного интерпретатора CIL кода. Мотивацией к данной работы послужил проект V#, в котором на данный момент используется символьное исполнения абстрактного синтаксического дерева C#, некоторые части которого было непонятно как правильно обрабатывать. Поэтому было принято решение решить эти проблемы интерпретируя инструкции CIL напрямую, что также позволить осуществлять верификацию всех программ, компилируемых в .NET.

В 1й главе "обзор" приводится общая схема алгоритма символьного исполнения, а также распространенные оптимизации и эвристики, которые применяются к данного рода алгоритмам, а именно стратегии слияния состояний и стратегия раскрутки рекурсии и циклов.

Во второй главе даются основные понятия, а также описание метода описания путей в графе. К сожалению, изложение ведется в виде набора теорем, поэтому понимание сути метода требует некоторых усилий. Автору следовало бы разбавить формальные выкладки неформальным описанием метода построения, и может быть даже примером построения для какой-нибудь программы.

В третьей главе представляется описание алгоритма символьного исполнения, который является доработкой алгоритма, упомянутого в обзоре. Главным отличием является то, что новый алгоритм по мере работы также строит уравнения на состояния программы, в то время как предыдущий занимался только поиском ошибок. Данная глава написана гораздо понятнее предыдущей, по-видимому автор потратил на неё гораздо больше времени.

В четвертой главе описываются детали реализации, в которых я не нашел ничего интересного.

В пятой главе проходит апробация предложенного подхода, который на данный момент умеет обрабатывать примерно 80% инструкций CIL. Пока не поддерживаются наборы инструкций, связанных с поддержкой исключений, что делает данный алгоритм не полным. Однако я думаю, что поддержка этих инструкций в символьном интерпретаторе вполне реализуема, едва ли предложенный подход окажется недееспособным на программах с исключениями.

По прочтению данной работы я не совсем понял, как именно используется в приведенном алгоритме так называемый concolic execution, описанный во введении.

В общем и целом автор предлагает интересный подход к верификации CIL кода, текущие недоработки я считаю исправимыми и отношусь к алгоритму в целом со

сдержанным оптимизмом. Полагаю, что проделанная работа вполне заслуживает звания бакалавра и оценки "отлично".

Косарев Дмитрий Сергеевич,
программист ООО "Интеллиджей Лабс"

Дата: 01 июня 2019 г

Подпись: _____