УДК 004.45

Методы и средства статического анализа исходного кода

Казакова Е.С.
Санкт-Петербург, Университет ИТМО
Научный руководитель – ассистент, Логинов И.П.
Санкт-Петербург, Университет ИТМО

Аннотация.
Программные ошибки могут привести к сбоям программ и появлению в них уязвимостей. Для их поиска применяются техники статического и динамического анализа. В данной работе рассмотрены инструменты, выполняющие статический анализ программ на нескольких языках программирования, а также исследуется возможность применения методов статического анализа кода к промежуточному представлению программ уровня сред выполнения.

Введение.
Для выявления ошибок в компьютерных программах применяются методы статического и динамического анализа кода. Динамический анализ программ позволяет выявить ошибки в поведении программы во время её выполнения. Реализуется такой анализ путем инструментирования специализированных инструкций в целевую программу, а также за счет моделирования состояния программы во время выполнения в виртуальной машине. В отличие от динамического анализа, методы статического анализа программ фокусируются на исходном коде программы. Такие методы реализуются на базе анализа графов потоков управления, потоков данных, проверки моделей (model checking).

Статический анализ кода выполняется за счет проверки его соответствия определенным критериям (правилам). Набор правил подразумевает покрытие ошибок определенного класса: проблемы в управлении и использовании памяти (использование “мертвых” указателей, наличие утечек памяти, обращений по нулевым указателям, переполнение буфера, выход за границы массивов), недопустимых арифметико-логических операций, ошибок типизации, использование неинициализированных переменных, некорректного использования библиотечных функций, и других. В данной работе исследуются техники статического анализа кода и инструментальное программное обеспечение, а также их применимость для анализа промежуточных представлений программ в контексте реализации двухстадийной модели компиляции.

Выводы.
Техники статического анализа кода позволяют выявить заданное подмножество ошибок, приводящих к проблемам безопасности. Применение техник статического анализа на уровне среды выполнения программ (к промежуточному представлению, например, CLR, LLVM) позволит гарантировать отсутствие данных ошибок вне зависимости от реализации компиляторов исходного языка.

Казакова Е.С. (автор) _____

Логинов И.П. (научный руководитель) _____