МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Государственное образовательное учреждение
высшего профессионального образования
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(государственный университет)

Разработка кроссплатформенного динамического анализатора бинарного кода на основе QEMU

Дипломная работа студента 919 группы ФРТК
Перова Максима Николаевича

Научный руководитель: кандидат военных наук,
доцент Семенихин Игорь Викторович

Москва 2015

Актуальность темы

- Компьютеризация
- Значительное число устройств, ПО которых не поставляется с исходным кодом
- Появление новых процессорных архитектур
- Развитие существующих архитектур

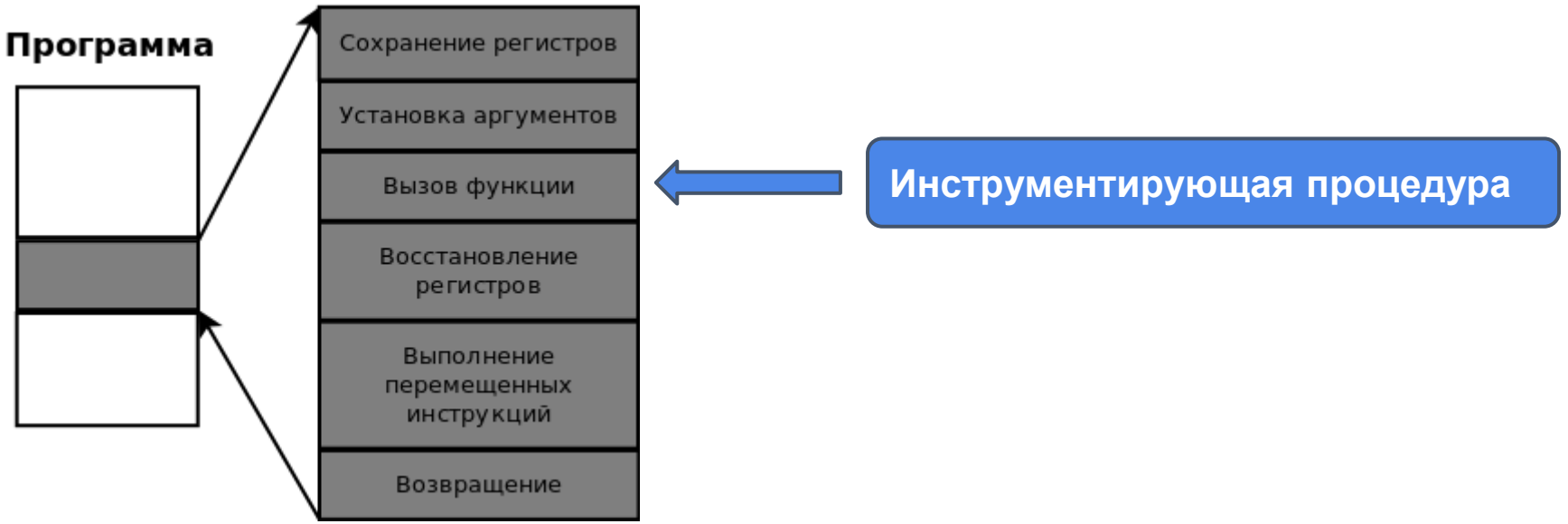
Цель и задачи работы

Цель дипломной работы – создание инструмента динамического анализа бинарного кода, поддерживающего множество архитектур, встраивание новой архитектуры в который будет происходить в полуавтоматизированном режиме.

Задачи:

1) Исследовать инструменты, основанные на технологии DBI.
2) Разработать инструмент идентификации переполнения буфера в стеке в бинарном исполняемом файле.
3) Разработать технологию автоматизации процесса встраивания новой архитектуры в QEMU.

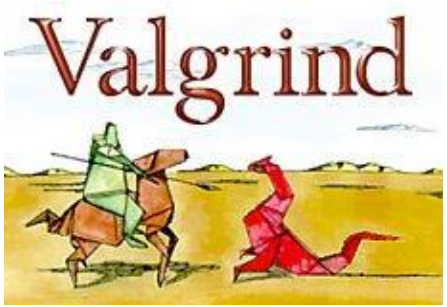
Dynamic Binary Instrumentation



Существующие решения

- Наиболее популярные
  - PIN
    - закрытый исходный код
  - Valgrind
    - малое количество поддерживаемых архитектур
    - анализ только прикладных программ
    - открытые исходные коды

- На основе QEMU
  - TEMU
    - больше не поддерживается
    - часть исходного кода закрыта
  - DECAF
    - не везде работает
    - открытые исходные коды



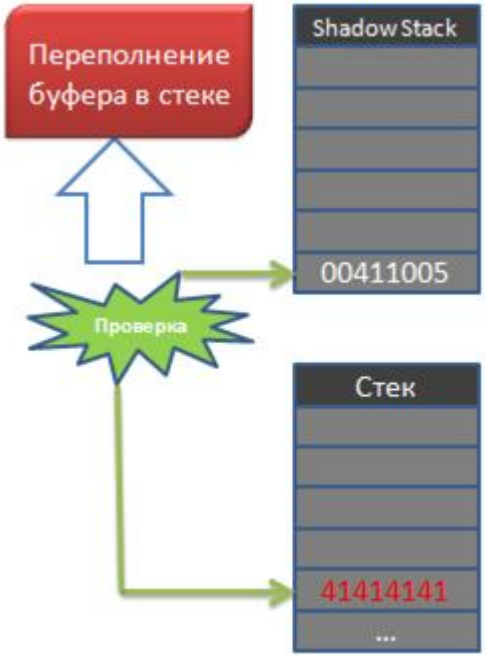
QEMU

- Трансляция кода в QEMU происходит при помощи Tiny Code Generator

- Для добавления новой архитектуры требуется только реализация трансляции гостевого набора инструкций в промежуточное представление

- Данное преобразование кода является **сюръективным** отображением.

Идентификация переполнения буфера

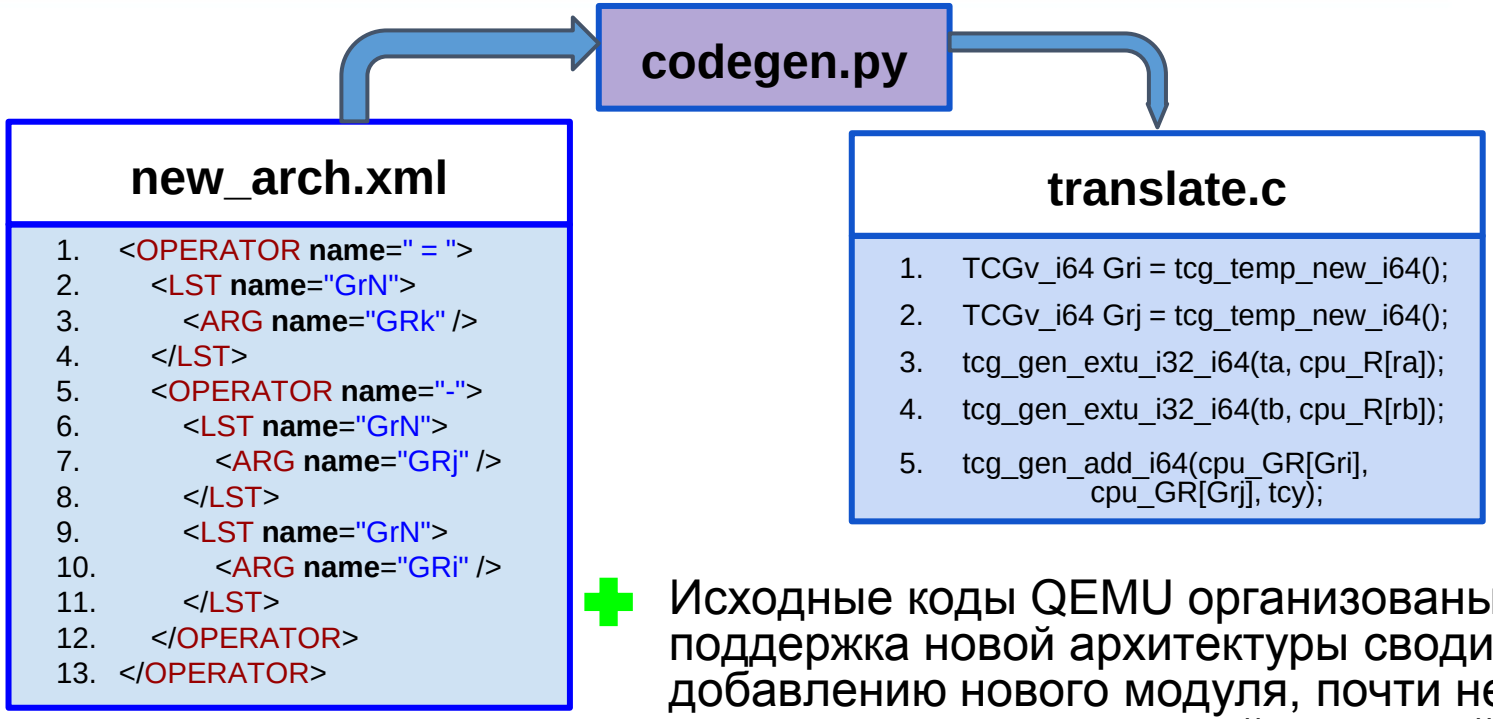


Единственная трудность:

в соответствии с преобразованием кода в QEMU, для каждого ***x*** необходимо найти соответствующий ***y***

x - инструкция гостевого кода
y - инструкция промежуточного кода

Добавление новой архитектуры



- Исходные коды QEMU организованы так, что поддержка новой архитектуры сводится к добавлению нового модуля, почти не затрагивая существующий исходный код

Результаты работы

- ✓ Описаны существующие инструменты динамического анализа бинарного кода
- ✓ Разработан инструмент идентификации переполнения буфера в стеке
- ✓ Реализована программа для встраивания новой архитектуры в QEMU
- ✓ Участие в 57-й научной конференции МФТИ
- ✓ Публикация на конференции «Комплексная защита информации»

В **аспирантуре** планирую разработать **DBI Framework** на основе QEMU.

Спасибо за внимание!