Санкт-Петербургский государственный университет

Кафедра системного программирования

Статистический анализ машинных инструкций

Афонина Ольга Андреевна, группа 22М.07-мм

Научный руководитель: старший преподаватель кафедры системного программирования СПбГУ, Я. А. Кириленко

Санкт-Петербург
2023

Введение

- Архитектуры процессоров постоянно развиваются, особый интерес представляет RISC-V, появляются новые расширения систем команд
- Необходимы оптимизации
  - аппаратные
  - оптимизации программного обеспечения
    - компиляторные
    - добавленные вручную
- Динамический анализ инструкций слишком трудоёмок и не гарантирует покрытие всей функциональности
- Необходимы агрегированные данные об использовании инструкций для различных утилит и платформ

Постановка задачи

Целью работы является разработка инструмента для статистического анализа машинных инструкций и создания обновляемого набора собираемых им данных.

Задачи:

- Провести обзор работ, применяющих статистический анализ использования машинных инструкций

Обзор: применения

- Выявление и классификация вредоносного кода
- Уменьшение потребляемой промежуточными представлениями памяти
- Подбор наименьшего числа приложений для проверки полноты бинарных утилит
- Переиспользование машинных кодов, занятых неиспользуемыми или устаревшими инструкциями

Обзор

Анализируемые данные:

- Частота инструкций
- N-граммы инструкций
  - на основе текста
  - на основе графа выполнения
- Дополнительные
  - используемые регистры
  - режимы адресации
  - размеры инструкций

Используемые инструменты:

- IDA Pro
- `objdump`

Обзор: выводы

- Есть потребность в наборе статистических данных использования инструкций
- В этом наборе необходимо предусмотреть возможность сохранения исходных результатов дизассемблирования
- Для сбора статистики в прототипе подойдёт утилита `objdump`

Результаты

- Проведён обзор методов применения статистического анализа машинных инструкций и выявлены подходящие для прототипирования решения

В рамках весеннего семестра планируется разработать прототип инструмента, воспроизведя результаты исследования, собравшего статистику для Ubuntu 16.04 и архитектуры x86-64, и расширив их на другие дистрибутивы и архитектуры.