Применение эмуляции для обратной инженерии

Вадим Евард
группа 445
руководитель М.В. Баклановский

Математико-механический факультет СПбГУ

5 сентября 2013 г.

Введение

Определения

- Обратная инженерия — исследование принципов работы системы по её структуре, функциональным возможностям и наблюдаемому поведению.
- Эмуляция — воспроизведение программными или аппаратными средствами либо их комбинацией работы других программ или устройств.

Подходы к анализу

- Статический
- Динамический
  - В «родном» окружении
  - В эмуляторе

Постановка задачи

- Исследовать возможности динамического анализа, предоставляемые эмулятором QEMU
- Получить статистики потока машинных команд, исполняемого в эмуляторе

Результаты и перспективы

- Анализ потока машинных команд
  - длина линейного участка: 5.14
  - длина блока трансляции: 5.11
  - 40% mov, 30% арифметика, 10% push/pop, переходы, сравнения
- Архитектура QEMU не предназначена для динамического анализа
- Возможное продолжение работы: QEMU+GDB, TEMU, Bochs