ПЛАТФОРМА ДЛЯ АНАЛИЗА ПРОГРАММ НА ОСНОВЕ ЭМУЛЯТОРА QEMU

Платформа ИСП РАН для анализа программ построена на базе открытого эмулятора QEMU, который используется при необходимости кросс-платформенной разработки. Поддерживает механизмы обратной отладки и интроспекции, а также режим полносистемной эмуляции для отладки низкоуровневого ПО.

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

QEMU поддерживает более 10 архитектур процессоров (i386 и Intel 64, ARM и Thumb, MIPS, PowerPC и др.). Реализует отладку по удаленному GDB-протоколу и совместим с IDA Pro, GDB и средами разработки. В режиме полносистемной эмуляции подходит для отладки низкоуровневого ПО — такого, как загрузчик и ОС. Исходный код QEMU систематически проверяется двумя статическими анализаторами (Coverity и Svace), что делает анализ потенциально вредоносного ПО в эмуляторе более безопасным.

Эмулятор с поддержкой обратной отладки и интроспекции доступен на GitHub: https://github.com/ispras/swat, как и набор инструментов автоматизации: https://github.com/ispras/qdt, https://github.com/ispras/i3s.

ПЛАТФОРМА ИСП РАН НА ОСНОВЕ QEMU — ЭТО:

- Запись и воспроизведение работы виртуальной машины:
  - При каждом воспроизведении виртуальная машина ведёт себя одинаково и точно так же, как при записи. Все воздействия извне зафиксированы и повторяются самим эмулятором, что упрощает отладку ошибок, связанных с параллельной работой приложения (состояние гонки, взаимные блокировки);
  - На базе воспроизведения реализована GDB-совместимая обратная отладка, которая заключается в откате к предыдущим снимкам состояния виртуальной машины и поиске предпоследнего срабатывания точки останова или предыдущей инструкции;
  - Записывается минимум информации, что позволяет вести длительную запись, необходимую для отладки редко повторяющихся ошибок;
  - Низкое относительное замедление, вносимое записью, позволяет контролировать ПО, требующее взаимодействия с удалённой системой в режиме реального времени.
- Получение высокоуровневой информации о работе гостевой ОС (интроспекция ВМ) без внесения каких-либо изменений в ядро ОС или установки программ мониторинга:
  - Возможность получить последовательность совершаемых системных вызовов, обращений к именованным функциям в динамических библиотеках, список работающих процессов, список открытых файлов и загруженных в память модулей;
  - Поддержка любого образа виртуальной машины на основе Linux, в том числе — образов встраиваемого ПО различных устройств;
  - Отладка с помощью встроенного в эмулятор сервера WinDbg, что позволяет отображать информацию о гостевом ПО в терминах абстракций ядра Windows. При этом не требуется включение отладочного режима работы гостевой ОС;

- Ускорение разработки расширений для QEMU:
  - Сокращение времени на подготовку средств динамического анализа для образцов кода, требующих специализированной аппаратуры;
  - Автоматизированное добавление процессорных архитектур с использованием генератора декодеров машинных команд и C-подобного языка описания семантики инструкций;
  - Система автоматического первичного тестирования виртуальной машины. Для работы системы требуются только утилиты GNU Binutils и компилятор языка C;
  - Автоматизированная разработка моделей устройств;
  - Генерация виртуальной машины (в форме исходного кода модуля QEMU) как из существующих, так и из новых устройств по описанию на языке Python с использованием графического интерфейса пользователя со схематичным изображением машины;
  - API для автоматизации процесса отладки на языке Python по протоколу GDB RSP: отладка гостевого кода, кода эмулятора и обоих одновременно.
- Удобство практического использования:
  - Свободное расширение возможностей QEMU благодаря открытому исходному коду и собственным инструментам ускоренной разработки ИСП РАН;
  - Анализ бинарного кода без внедрения программ в гостевую систему;
  - Модульная структура механизма интроспекции с возможностью расширения за счёт новых плагинов;
  - Удобное API для самостоятельной разработки плагинов интроспекции;
  - Возможность адаптации под конкретные нужды пользователя;
  - Поддержка актуальных версий QEMU с новой периферией и процессорными ядрами.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА ПЛАТФОРМА НА БАЗЕ QEMU?

- Разработчики загрузчиков, драйверов, ОС и другого системного ПО;
- DevOps-команды (воспроизводимость ошибок, кросс-разработка, масштабирование тестирования в облачной среде);
- Аналитики потенциально вредоносного ПО;
- Специалисты по сертификации ПО.

ПОДДЕРЖИВАЕМЫЕ ГОСТЕВЫЕ СРЕДЫ

Эмулируемые платформы: i386, x86-64, ARM, MIPS, PowerPC и другие.
Гостевые системы, поддерживаемые интроспекцией: Windows XP (x86), Windows 10 (x86-64) и Linux 2.x-4.x на платформах x86, x86-64, ARM, AArch64.

ОПЫТ ВНЕДРЕНИЯ

Реализованный механизм воспроизведения принят мировым сообществом разработчиков QEMU и включен в версию 3.1.

СХЕМА РАБОТЫ