ТРАЛ: СРЕДА АНАЛИЗА БИНАРНОГО КОДА

ТРАЛ – уникальный промышленный инструмент для анализа свойств бинарного кода. Позволяет работать с кодом различных целевых процессорных архитектур. Не требует наличия отладочной информации и исходных кодов. Применим для анализа всего программного стека от загрузчика до прикладного ПО. Включён в Единый реестр российского ПО (№5323).

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

ТРАЛ – комплекс технологий, основанный на многолетнем опыте разработчиков компиляторов и специалистов по информационной безопасности. В отличие от аналогичных научно-исследовательских технологий в области анализа бинарного кода, доработан до промышленного использования.

Ключевые возможности:

- полносистемный анализ бинарного кода, исследуется весь стек развернутого ПО;
- восстановление потоков данных и управления на уровне машинных команд;
- локализация в коде отдельных алгоритмов, формальное представление их структуры и семантики;
- выявление утечек чувствительных данных по памяти на основе динамического анализа помеченных данных по полносистемным трассам выполнения;
- автоматизация экспертизы исполняемого кода.

ТРАЛ – ЭТО:

- Модульная архитектура, которая позволяет расширять набор поддерживаемых целевых платформ и развивать функциональное наполнение.
- Поддержка автоматизации анализа с помощью сценариев и открытого API.
- Интеграция с другими инструментами: Radare2, QEMU, IDA Pro и Wireshark.
- Глубокий анализ:
  - для анализа достаточно наличия лишь исполняемого бинарного кода;
  - в основе подхода – динамический анализ, при необходимости дополняемый статическим анализом снимков памяти;
  - предварительное автоматическое повышение уровня представления бинарного кода;
  - восстановление статического представления программ, входящих в состав анализируемой системы, в т. ч. по нескольким запускам;
  - точный анализ потоков данных, учитывающий особенности аппаратуры (конвейер команд, прерывания, трансляция виртуальных адресов, DMA);
  - интерактивное восстановление блок-схемы алгоритма, основанное на построении срезов информационных потоков;
  - подход, реализованный в среде, невосприимчив к большинству известных приёмов противодействия анализу.
- Высокая производительность:
  - параллельный анализ с высокими показателями масштабируемости на многоядерных рабочих станциях;
  - возможность анализа длительных сценариев работы анализируемой системы.
- Развитый графический интерфейс:
  - просмотр трасс выполнения с обширными возможностями поиска и навигации, аналогичными классическому отладчику, но с возможностью мгновенного перемещения по потокам данных как вперёд, так и назад во времени;

- автоматическая разметка высокоуровневой структуры трассы: процессов и потоков выполнения, обработчиков прерываний, стеков вызовов, динамически загружаемых модулей и символов в них;
- просмотр значений параметров и возвращаемых значений вызванных функций;
- разметка трассы с указанием внешних событий (сетевые взаимодействия и пользовательский ввод-вывод) и событий, связанных с работой аппаратуры;

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ТРАЛ?

Государственные учреждения, в обязанности которых входят исследования безопасности программного обеспечения.

УСЛУГИ С ИСПОЛЬЗОВАНИЕМ ТРАЛ

- Исследования программного обеспечения при проведении сертификации.
- Целевое обучение и повышение квалификации сотрудников государственных учреждений.

АДАПТАЦИЯ И РАЗРАБОТКА ПРОБЛЕМНО-ОРИЕНТИРОВАННЫХ РЕШЕНИЙ НА БАЗЕ ТРАЛ

- Для государственных учреждений.
- Для компаний-разработчиков встраиваемого ПО и компонентов ОС.
- Для компаний-разработчиков безопасного/доверенного ПО.
- Для компаний, проводящих анализ вредоносного кода.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

- Системные требования среды анализа ТРАЛ: ОС Windows или ОС на базе ядра Linux, 64-разрядный процессор архитектуры x86, 16 и более ГБайт ОЗУ.
- Целевые процессорные архитектуры: x86, x86-64, ARMv6, ARMv7.
- Целевые ОС: семейство Windows, семейство Linux, поддерживается возможность работы с неопознанной ОС и с кодом, работающим вне ОС.

СХЕМА РАБОТЫ