BINSIDE: СТАТИЧЕСКИЙ АНАЛИЗАТОР БИНАРНОГО КОДА

BinSide — инструмент обнаружения дефектов в программе методами статического анализа исполняемого кода. Необходим, когда нет доступа к исходному коду (например, при анализе закрытых библиотек).

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

BinSide — платформа для анализа бинарного кода, разрабатываемая на основе фреймворка BinNavi, который переводит ассемблерный код в представление REIL. Данное представление позволяет анализировать код независимо от процессорной архитектуры и операционной системы. Интегрирован с дизассемблерами IDA PRO и Ghidra, которые используются для обратной разработки.

ВОЗМОЖНОСТИ ЯДРА BINSIDE

- Лёгкая расширяемость:
  - детекторы ошибок реализованы в виде подключаемых модулей;
  - используется представление REIL из 17 инструкций без побочных эффектов (каждая ассемблерная инструкция транслируется в набор из REIL-инструкций).
  - возможность разметки для функций источников распространения помеченных данных.
- Поддерживает анализ бинарных файлов и библиотек для архитектур x86-64, ARM и MIPS.
- Поиск дефектов типа: CWE-121 (Stack-based Buffer Overflow), CWE-122 (Heap-based Buffer Overflow), CWE-134 (Use of Externally-Controlled Format String), CWE-415 (Double Free), CWE-416 (Use After Free).
- Ядро анализа позволяет выполнять:
  - анализ значений и указателей;
  - отслеживание помеченных данных, моделей статической и динамической памяти, а также анализ с учётом потока данных и управления;
- поиск ошибок на всех путях (в том числе не покрытых тестированием или динамическим анализом).
- Возможность конвертировать результаты в формат Svace (при наличии отладочной информации) для отображения в веб-интерфейсе в целях навигации по исходном коду;

КОМПОНЕНТЫ BINSIDE:

- Компонент восстановления семантики функций;
- Компоненты на базе технологии поиска клонов кода:
- Компонент libraryIdentifier:
  - обнаружение использования устаревших версий библиотек;
  - определение нарушений авторских прав.
- Компонент для анализа изменений между версиями программ;
- Компонент переноса разметки имён функций с одного бинарнаго файла на другой.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН BINSIDE?

- Компании, которые нуждаются в тщательной проверке стороннего ПО при отсутствии доступа к исходному коду;
- Разработчики, которым требуется повысить качество работы инструментов динамического анализа за счёт дополнительных данных, полученных с помощью статического анализа.

СХЕМА РАБОТЫ