KLEVER: ТЕХНОЛОГИЯ ВЕРИФИКАЦИИ МОДЕЛЕЙ КРУПНЫХ ПРОГРАММНЫХ СИСТЕМ

ИСП РАН

Klever — система верификации моделей, которые генерируются на основе исходного кода крупных программных систем, разработанных на языке программирования Си. Klever позволяет автоматизированным образом проверять различные требования безопасности и надёжности.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Klever базируется на научных исследованиях в области выполнения полностью автоматического доказательства корректности моделей программ, извлекаемых из исходного кода (в том числе без участия пользователя). В основе системы лежат методы для покомпонентной верификации исходного кода программных систем размером в сотни тысяч и миллионы строк кода на языке Си. Klever выложен в открытый доступ (https://forge.ispras.ru/projects/klever).

KLEVER — ЭТО:

- Высокоточный консервативный анализ исходного кода индустриального программного обеспечения (выявление всех возможных ошибок искомых видов и доказательство корректности программ при явно заданных предположениях).
- Проверка расширяемого набора требований к программе (проверка правил безопасного программирования на языке Си и корректности использования программных интерфейсов, специфичных для проверяемых программ).
- Масштабируемость. Модульная верификация программ позволяет применять наиболее точные методы для анализа больших объёмов исходного кода (в частности, методы верификации моделей и символьного выполнения).
- Подробные сведения об обнаруживаемых ошибках. Система верификации не только указывает на места ошибок в исходном коде, но также предоставляет последовательности выражений и значения переменных и аргументов функций для их воспроизведения.
- Удобный многопользовательский веб-интерфейс для проведения верификации, а также для выполнения экспертной оценки результатов верификации;
- Возможность адаптации системы верификации под конкретные нужды заказчиков. Разработка наборов спецификаций для обнаружения нарушений специфичных для программ требований, включая моделирование специфичных окружений целевых программ.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН KLEVER?

- Компании, нацеленные на разработку ПО с высоким уровнем надёжности и безопасности;
- Испытательные лаборатории.

ОПЫТ ВНЕДРЕНИЯ

Klever разработан в рамках работы Центра верификации ОС Linux (http://linuxtesting.org/), организованного на базе ИСП РАН при поддержке The Linux Foundation. В настоящее время система верификации в основном применяется для различных операционных систем.

Для демонстрации возможностей Klever были выполнены работы по верификации драйверов устройств ядра операционной системы Linux. В результате удалось обнаружить более

350 ошибок, подтверждённых разработчиками: ошибки выхода за границу буфера, разыменование нулевого указателя, использование неинициализированной памяти, повторное или некорректное освобождение памяти, состояния гонки и взаимные блокировки, утечки специфичных ресурсов ядра Linux, некорректные вызовы функций в зависимости от контекста, некорректная инициализация структур данных ядра Linux.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Ubuntu 18.04, 16 гигабайт оперативной памяти, от 100 Гб свободного места на диске.

СХЕМА РАБОТЫ