СИСТЕМА ВЕРИФИКАЦИИ
ASTRAVER TOOLSET

AstraVer Toolset — система дедуктивной верификации ключевых компонентов. Позволяет разрабатывать и верифицировать модели политик безопасности, а также проводить доказательство корректности компонентов на языке C. Необходимый инструмент достижения целей семейств доверия ADV_SPM и ADV_FSP, определённых в ГОСТ Р ИСО/МЭК 15408-3-2013.

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

AstraVer Toolset — комплекс инструментов, предназначенный для промышленного использования и основанный на многолетних научных исследованиях. Объединяет два подхода к верификации: на уровне моделей и на уровне кода. Решает те же задачи, что и аналогичные инструменты (Microsoft VCC, Frama-C WP), однако благодаря специфической доработке обладает технологической уникальностью: возможностью верификации ключевых компонентов системы безопасности ядра Linux. Выложен в открытый доступ (http://linuxtesting.ru/astraver).

ASTRAVER TOOLSET — ЭТО:

- Комплексный подход к верификации, начиная с формализации требований верхнего уровня и до анализа поведения кода.
- Моделирование функциональных требований (формализация функциональных требований к системе, доказательство внутренней согласованности требований и недостижимости небезопасных состояний).
- Тестирование реализации на соответствие функциональным требованиям с использованием формальной модели требований для проверки корректности наблюдаемого поведения в целях оценки качества тестирования и генерации тестов.
- Верификация ключевых компонентов на языке C (формализация требований к ключевым компонентам, доказательство корректности работы компонента на всех возможных входных данных).
- Поддержка индустриального кода (нестандартные расширения компилятора GCC, арифметические операции с побитовой точностью, адресная арифметика (включая поддержку конструкции container_of), функциональные указатели, приведение целочисленных типов к указательным).
- Решение важнейших задач профилей защиты:
  - формальное моделирование политики безопасности;
  - формальное доказательство внутренней непротиворечивости модели политики безопасности и недостижимости небезопасных состояний;
  - разработка полуформальной или формальной функциональной спецификации;
  - формальное или полуформальное доказательство соответствия между моделью политики безопасности и функциональной спецификацией;
  - формальное или полуформальное доказательство соответствия между различными представлениями целевого ПО, такими как функциональная спецификация, проект ПО и его реализация.
- Возможность доработки комплекса под конкретного заказчика (в плане поддержки верификации компонентов на языке C).

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ASTRAVER TOOLSET?

- Компании, нацеленные на разработку ПО с высокой степенью надёжности и безопасности — как информационной, так и функциональной (ПО для самолётов, АЭС и др.);
- Компании, которые нуждаются в сертификации разрабатываемого ПО в соответствии с ГОСТ Р ИСО/МЭК 15408;
- Испытательные лаборатории средств защиты информации в соответствии с требованиями безопасности.

ОПЫТ ВНЕДРЕНИЯ

Система AstraVer Toolset применялась при разработке средств защиты информации ОС Astra Linux Special Edition (АО «НПО РусБИТех»), которая успешно прошла сертификацию на соответствие требованиям безопасности информации ФСТЭК России к операционным системам по профилю защиты «2А». В основу отечественной разработки была положена МРОСЛ-ДП модель безопасности, а реализация ее новых возможностей в ОС Astra Linux Special Edition продолжает верифицироваться с помощью AstraVer Toolset.

СХЕМА РАБОТЫ