РБПО как фундамент жизненного цикла ОС Нейтрино

Дужак Евгений Дмитриевич, ООО «СВД ВС», г. Санкт-Петербург ул. Кузнецовская д. 19, e.duzhak@kpda.ru

Изоляция процессов в ОС «Нейтрино»

ЗОСРВ «Нейтрино» - микроядерная система. Изоляция процессов один из базовых принципов, лежащих в основе ее архитектуры. Каждый программный модуль, включая и драйверы, выполняется в собственном изолированном адресном пространстве и таким образом, все драйверы устройств, стек TCP/IP, пользовательские программы - это независимые процессы, которые взаимодействуют через микроядро и включаются в состав целевой системы по необходимости.

Изоляция процессов как механизм обеспечения безопасности ОС

Изоляция процессов в ЗОСРВ «Нейтрино» гарантирует защиту памяти: ни одно приложение не может случайно или умышленно получить доступ к данным другого процесса или изменить их.

Такая изоляция выступает одной из базовых функций безопасности системы. Безопасность всей ОС строится на надёжности каждого её компонента — от ядра до прикладных приложений. Создание действительно защищённой и доверенной системы невозможно, если безопасность не закладывалась с самого начала разработки.

Комплексный подход требует интеграции механизмов верификации и контроля на всех этапах: проектирование архитектуры, написание кода, тестирование и эксплуатация.

Жизненный цикл ОС «Нейтрино»

Безопасная разработка ЗОСРВ «Нейтрино» представляет собой конвейер, отправной точкой которого является доверенный и изолированный git-репозиторий. В репозиториях строго зафиксирован состав релизных версий ОС (в том числе и для opensource-компонентов). Далее в рамках закрытого сборочного сервера, защищенного сетевым экраном, с помощью CI/CD системы, производится компиляция с помощью контейнеров с установленным и верифицированным сборочным окружением, на данном этапе проводятся те виды анализа, которые не требуют исполнения(например, статический анализ кода). Другие же виды анализа проводятся в рамках тестового стенда. Завершением сборки ОС – является этап публикации сборочных и верификационных артефактов на внутренний ресурс, для последующего анализа.

ОС делится на подсистемы не только как код, но и как проект. За каждый проект(подсистему) ответственна команда разработчиков. Проект управляется через систему управления проектом.

В процессе разработки ОС используются следующие технологии:

Статический анализ. Для проведения СА сформирован регламент, согласно которому статический анализ проводится в рамках принятия изменений в код(PR/MR), а также раз в неделю для сборки верификационного билда ОС.

Динамический анализ – фаззинг-тестирование, функциональное и модульное тестирование, системный анализ – объектом исследования данными методами становится верификационный билд ОС. Исходными данными для первоочередных целей для фаззинг-тестирования является поверхность атаки ОС.

Композиционный анализ – ОС - многокомпонентный продукт, поэтому часть компонентов использует opensource-код. Композиционный анализ решает проблему поиска

уязвимостей по открытым базам уязвимостей. Вопрос поиска внедрения каких-либо сторонних компонентов на этапе сборки в случае ОС «Нейтрино» не является актуальным, так как она собирается в замкнутом изолированном контуре (реализуется docker-контейнером) с помощью конкретных версий компиляторов путем кросс-компиляции.

CI/CD – используется для организации обратной связи в рамках построения дистрибутива, его верификации и сбора информации обо всех процессах, с последующей публикацией на внутренних ресурсах.

Некоторые технологии для ЗОСРВ «Нейтрино» могут использоваться напрямую без адаптации, например средства статического анализа, композиционного анализа или системы CI/CD. Динамический анализ зависит от компиляторов, которые для ЗОСРВ «Нейтрино» отличаются от других операционных систем, поэтому готовых решений не было. В рамках рабочего процесса были взяты доступные, одобренные сообществом РБПО, opensource технологии, которые в последствии адаптировались для использования в ЗОСРВ «Нейтрино».