Автор

Бондарев Антон Владимирович
Embox

Аннотация

В соврменнном мире требования к безопасности цифровых системы постоянно увеличиваются. Цена ошибки при нарушении уровня безопасности растет с каждым этапом жизненного цикла продукта. Поэтому при разработке конечных систем стремятся улучшить ее безопасность, на как можно более ранних этапах, в идеале еще на этапе проектирования системы.

В докладе будет рассмотрен подход основанный на описании требований к системе на этапе проектирования позволяющий улучшить безопасность и надежность конечной системы. Данный подход применяется в проекте открытой ОСВР Embox

Тезисы

Современные системы становятся все более “умными” и от них ожидают все большего функционала. Вместе с увеличением функциоанльности все острее встает вопрос о безопасности и надежности современных систем.

Существуют разные подходы к увеличению безопасности и надежности ПО доказавшие свою эффективность: использования языков программирования высокого уровня, использование анализаторов кода, использование различных видов тестирования и так далее. Наибольшего эффекта можно достичь, если проецесс разрыботкис будет включать необходимые части. Причем сам процесс должен включать требования к качеству, недежности и безопасности конечного продукта.

Одним из способов уменьшить противорение между растущей функциональностью и требованием обеспечения надежности и безопасности, является ограничение функциональности системы только той которая используются. И максимальная проверка конечной функциональности на этапе проектирования системы.

Это можно достичь, если использовать специальный язык на котором можно описать как желаемые характеристики конечной системы, так и характеристики отдельных модулей.

Системе сборки ОС РВ Embox использует специализированного языка (DSL) описания модулей (Mybuild) которые описывает, все части модули включая ядерные и прикладные, а также статически заданные требования к конечной системе. На основе этих требований и описаний модулей, строится внутренняя модель (граф) системы, которая анализируется статически, сквозным образом.

В процессе сборки Embox создает свое уникальное программное окружение, включающем, такие части как характеристики и функции ядра, необходимые функции для требуемых подсистем (файловая, сетевая и так далее), стандартная библиотека и остальные необходимые части необходимые для корректной функциональности конечной системы.

Таким образом получается конечный образ имеющий всю необходимую функциональность, но исключающую другую. Получаемое программное окружение является уникальным и не совместимым для других конфигураций системы. Что позволяет исключить запуск зарегистрированного в процессе проектирования ПО, резко уменьшить количество строчек кода и функциональность которая нуждается в проверке.

В докладе рассматривается система сборки проекта Embox: внутренняя организация, получаемые характеристики, синтаксис языка Mybuild, примеры использования.