Создание критически важных приложений на основе микросервисов.

Журнал: “Открытые системы СУБД” , номер 1, 2017 год.
Издатель: ООО “Россия, 127254, Москва”.

Кристоф Фетцер

Стандартный подход к созданию ответственных приложений для бизнеса и критически важной инфраструктуры — это подход «снизу вверх», когда начинают с надежного фундамента, выбирая аппаратную архитектуру и системное ПО, а поверх него разрабатывают приложение и обеспечивают его безопасное выполнение. Убедиться в надежности микропрограммного и системного ПО (ОС, гипервизор, диспетчер ресурсов и т. д.) помогают формальные методы доказательства корректности микроядерной системы .

Под управлением Linux, операционной системы с монолитным ядром, сегодня работают многие современные системы и устройства: облачные инфраструктуры, смартфоны, автомобильные компьютеры и другие устройства, критичные к безопасности встроенного программного обеспечения . Однако доказать корректность работы ОС Linux современными формальными методами практически нереально — если в самом микроядре насчитывается лишь 10 тыс. строк кода, то для ядра Linux пришлось бы верифицировать более 20 млн строк. Более того, опыт показал, что Linux всегда содержит исправимые ошибки, так что формальное доказательство корректности в любом случае даст отрицательный результат.

Статический анализ репозиториев открытого кода обычно выявляет в среднем 0,61 дефекта на тысячу строк, и, несмотря на постоянно проводимые исправления, число неустраненных ошибок в ядре остается на уровне примерно 5 тыс. ; правда, не все они могут использоваться для проведения атак. Другое исследование показало, что за последние пять лет в Linux было исправлено около 500 ошибок, связанных с нарушением безопасности, и они присутствовали в ядре в течение пяти лет.