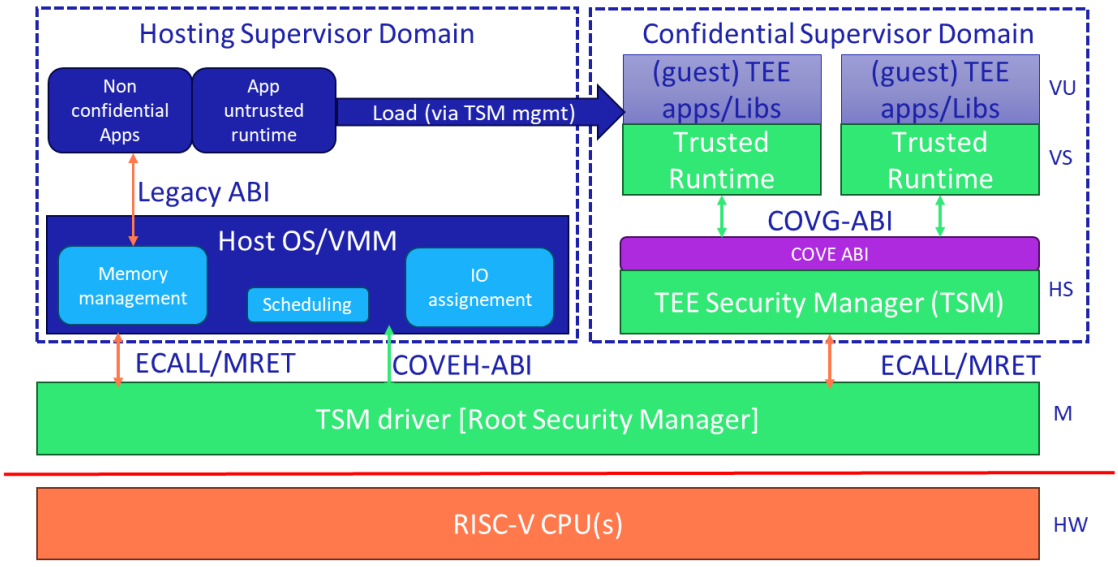
"Конфиденциальное расширение виртуальной машины (CoVE) для безопасных вычислений на платформе RISC-V "

В последние несколько лет облачные вычисления приобрели очень большую популярность во многих областях: от логистики и ритейлеров, до турфирм и банков. Очень многие коммерческие организации предпочитают строить бизнес на арендованных серверах и не тратить свои ресурсы на поддержание инфраструктуры. Сохранение конфиденциальности информации в облачных вычислениях, наряду с доступностью сервисов, играет ключевую роль в этом направлении.
С выходом архитектуры RISC-V на серверный рынок функции программной и аппаратной защиты конфиденциальности виртуальных машин приобретают первостепенное значение. В качестве реакции на эти вызовы RISC-V сообщество предложило и активно развивает расширение конфиденциальной виртуальной машины – CoVE/CoVE IO (Confidential Virtual Machine extension).

Мы расскажем об интерфейсе конфиденциального расширения виртуальной машины (CoVE) для масштабируемой доверенной среды выполнения (TEE) для случая аппаратных рабочих нагрузок на основе виртуальных машин на платформах, основанных на RISC-V архитектуре. Это расширение позволяет рабочим нагрузкам приложений, требующим конфиденциальности, сократить доверенную вычислительную базу (TCB) до минимального размера, в частности, оставляя хостовую ОС/VMM и другое программное обеспечение вне доверенной вычислительной базы.

Расширение описывает изолированный (конфиденциальный) домен супервизора для обеспечения соблюдения свойств доверенной вычислительной базы и конфиденциальности при использовании изолированного домена супервизора для домена хоста, таким образом сохраняя роль доменом супервизора хостинга (OS/VMM) в качестве менеджера ресурсов (как для устаревших виртуальных машин, так и для доверенных виртуальных машин). Ресурсы, управляемые доменом супервизора хостинга, включают память, ЦП, ресурсы ввода-вывода и возможности платформы для размещения рабочей нагрузки доверенной виртуальной машины.



Решение основано на изоляции физических страниц памяти на основе аппаратной реализации таблиц отслеживания памяти (SmMTT). Остальная часть расширения является программной и может быть легко адаптирована на различные аппаратные реализации на платформе RISC-V.