КОНФИДЕНЦИАЛЬНОЕ РАСШИРЕНИЕ ВИРТУАЛЬНОЙ МАШИНЫ (COVE) ДЛЯ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ НА ПЛАТФОРМЕ RISC-V

Июнь, 2024

Константин Невидин

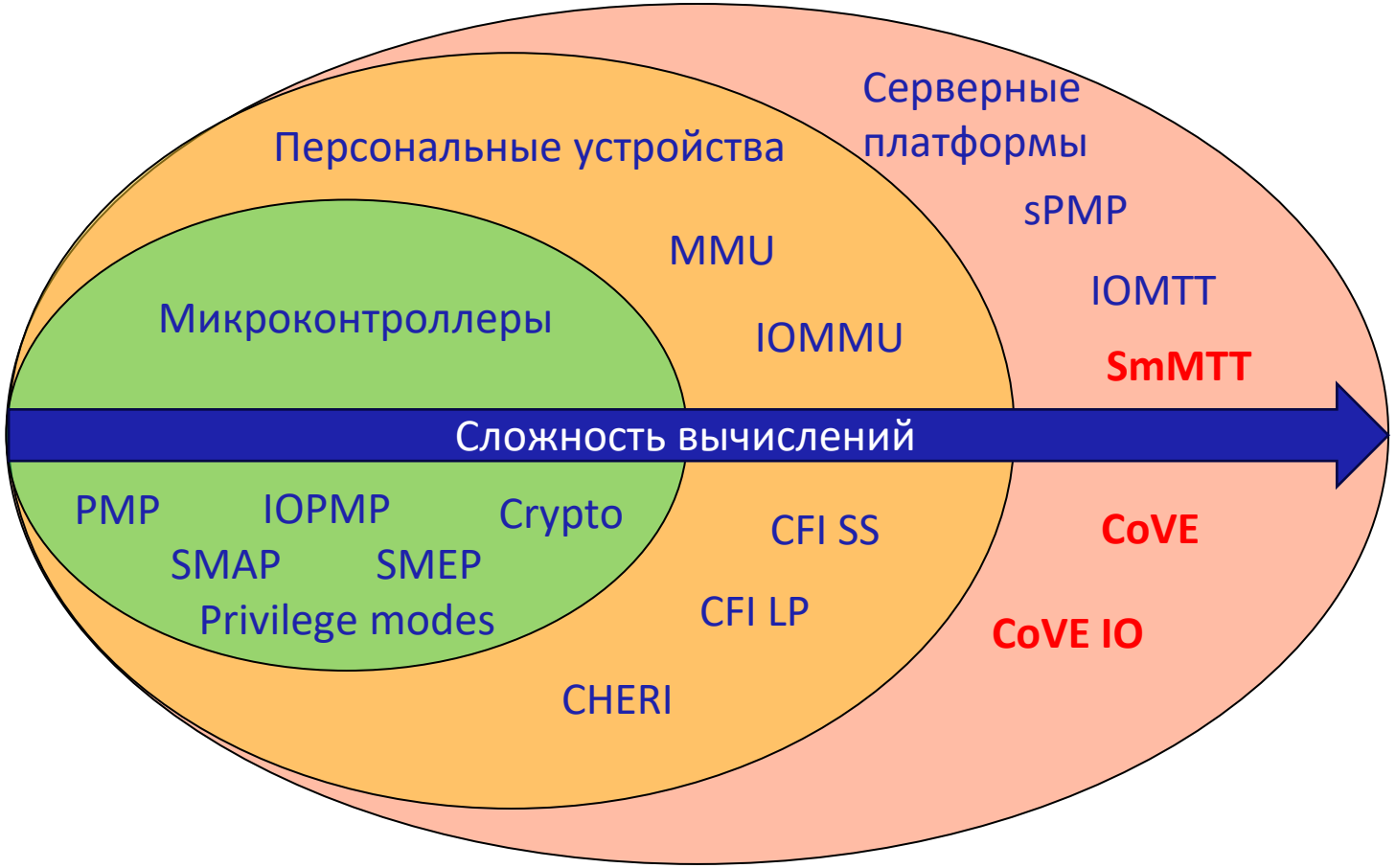
Введение в проблему

Таблица отслеживания памяти супервизора (SmMTT)

Конфиденциальное расширение виртуальной машины (CoVE)

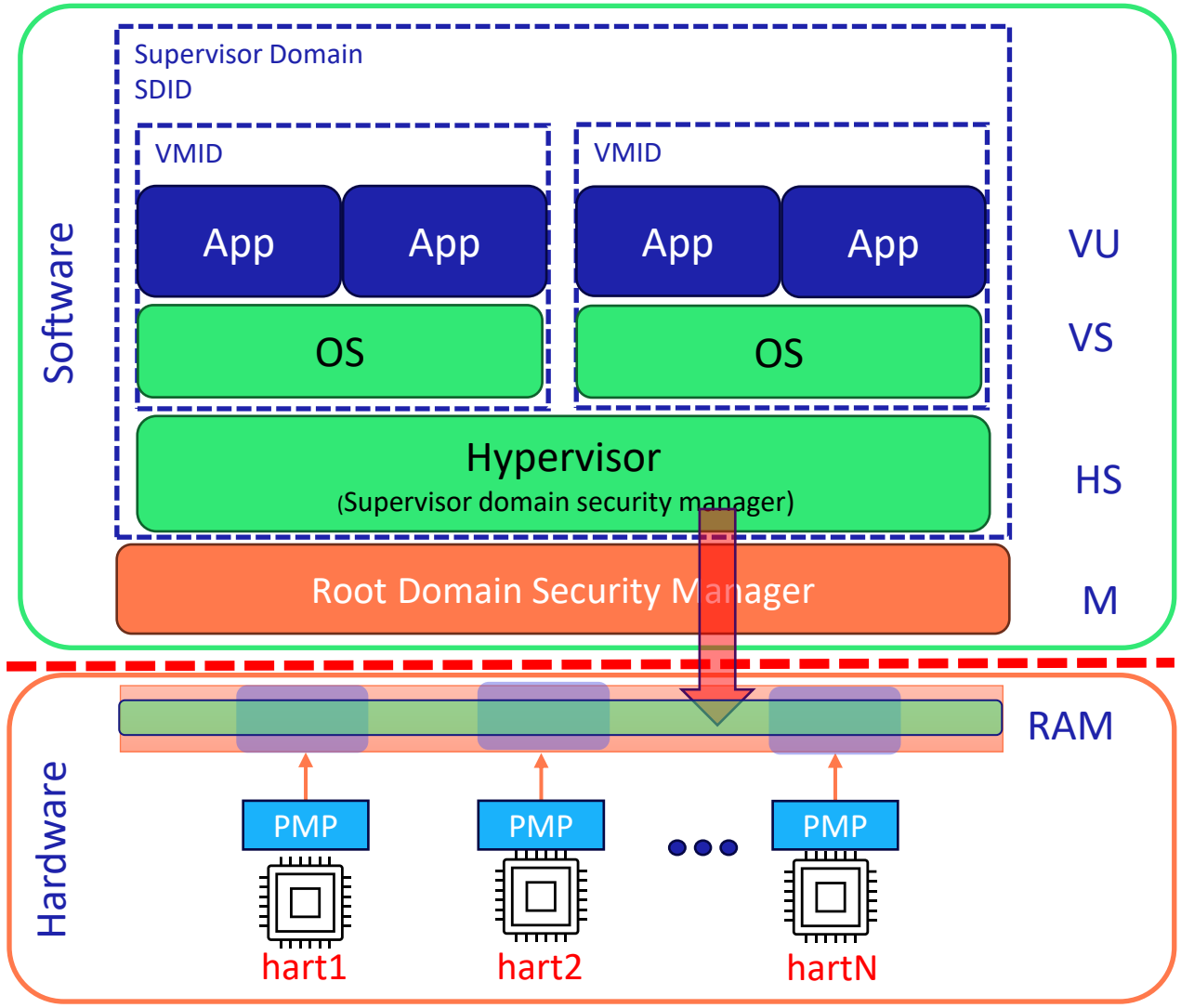
Работа с внешними устройствами в конфиденциальном расширении виртуальной машины

Развитие средств защиты в архитектуре RISC-V



PMP – Physical Memory Protection
IO – input/output
MMU – Memory management unit
SMAP/SMEP – Supervisor Memory Access/Execution Prevention
CHERI – Capability Hardware Enabled RISC-V Instructions
CFI – Control flow integrity
SS – Shadow Stack
LP – Landing pads
sPMP – Supervisor mode PMP
SmMTT – Supervisor mode Memory Tracking Table
CoVE - Confidential VM Extension

Изоляция приложений, ОС, супервизора

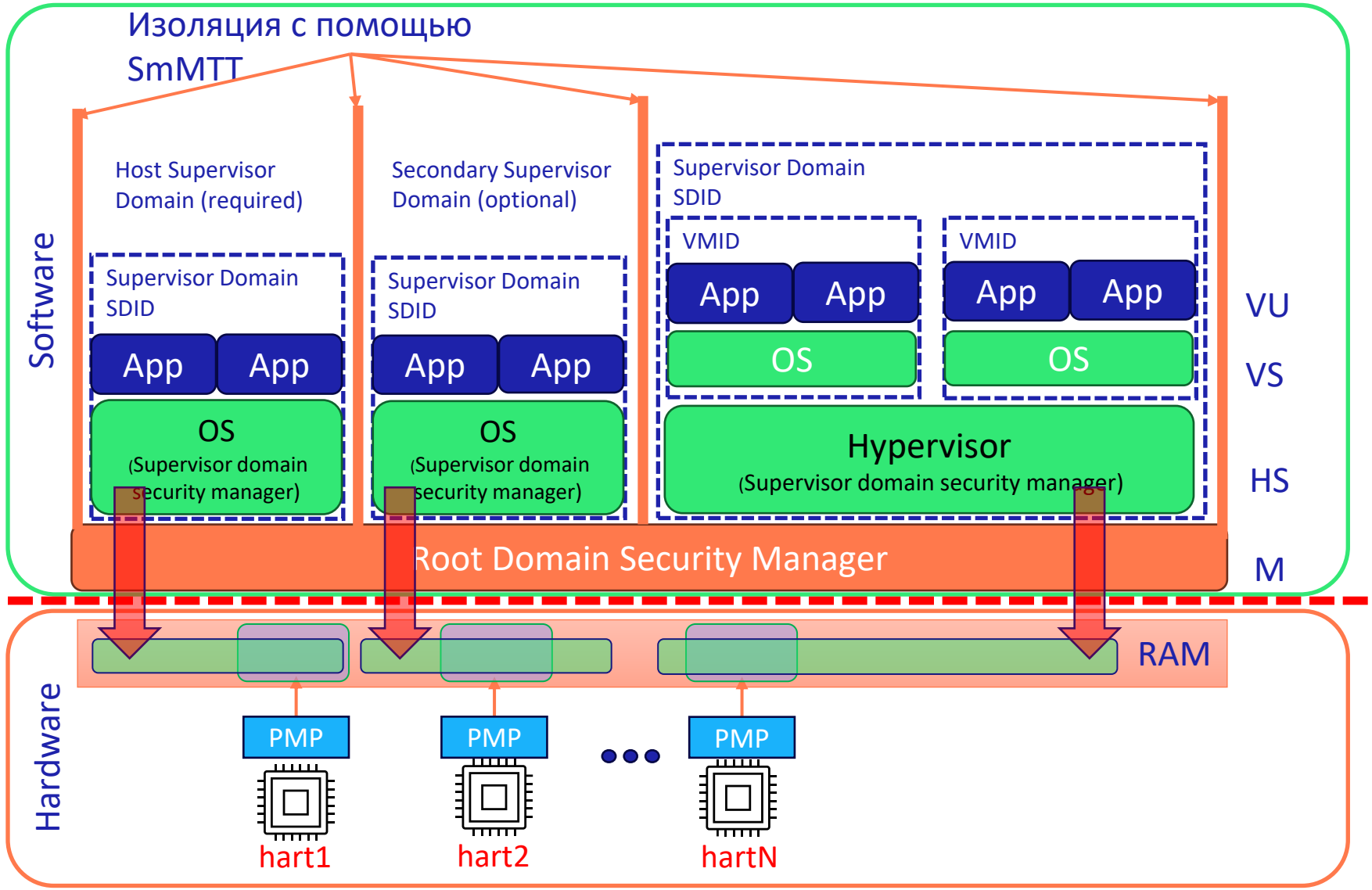


Проблема:
Гипервизор имеет доступ ко всей физической памяти и внешним устройствам

Как разграничить доступ к памяти для нескольких гипервизоров?

Smsdid

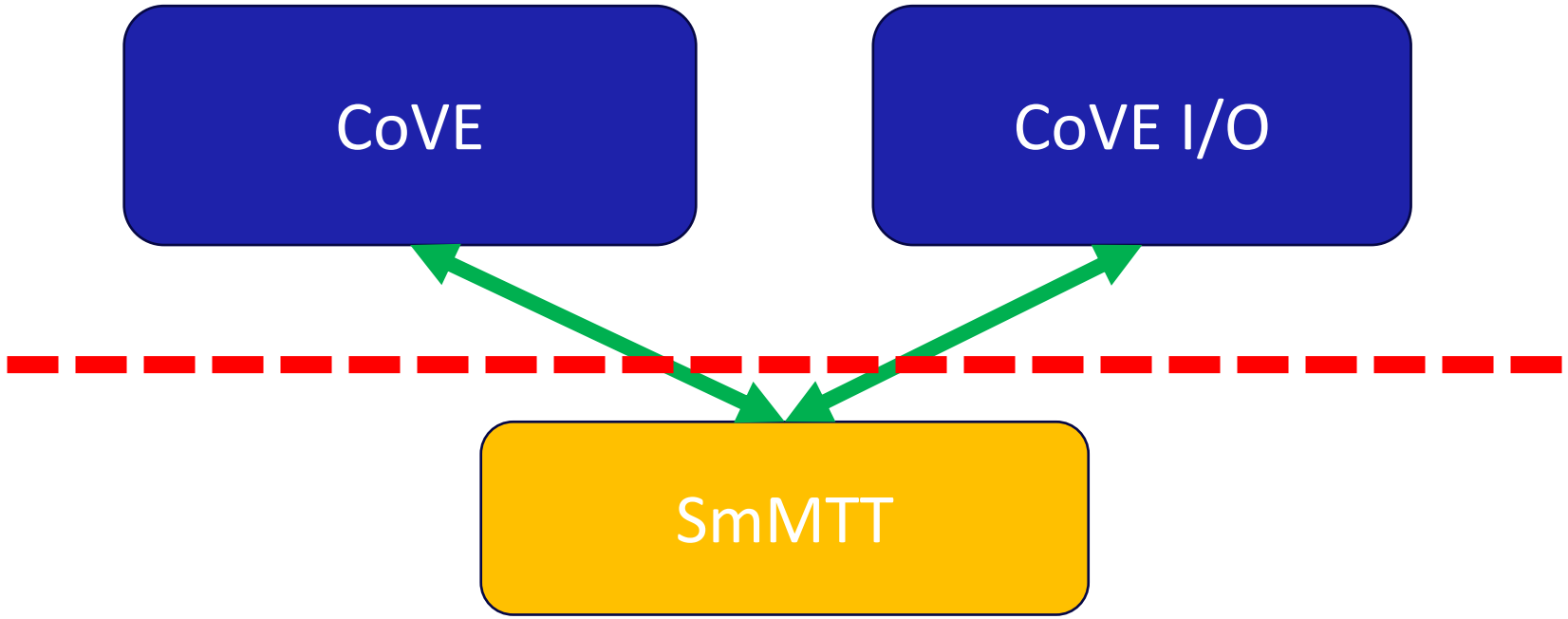
Изоляция между доменами супервизора



- Только RDSM имеет доступ ко всему физическому адресному пространству.
- Идентификатор домена супервизора (SDID) связан с доменом супервизора.
- Домен супервизора связан с набором регионов физических адресов, которые изолированы от других доменов супервизора на той же платформе

Расширение конфиденциальной виртуальной машины- CoVE, CoVE IO, SmMTT

Non-ISA
Софтверная
реализация

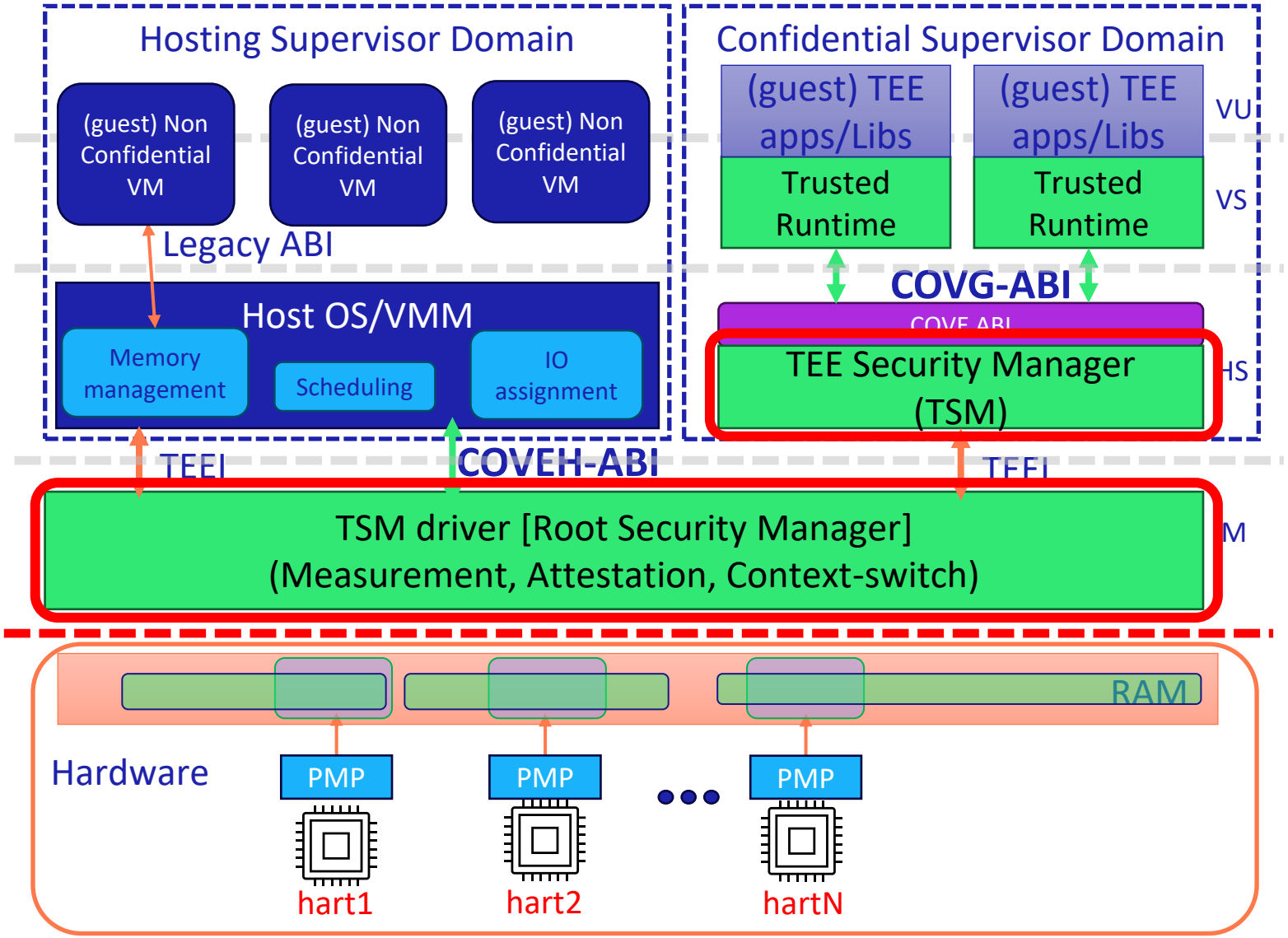


ISA –
изменения в
железе

SmMTT - назначение таблицы отслеживания памяти для изоляции домена супервизора

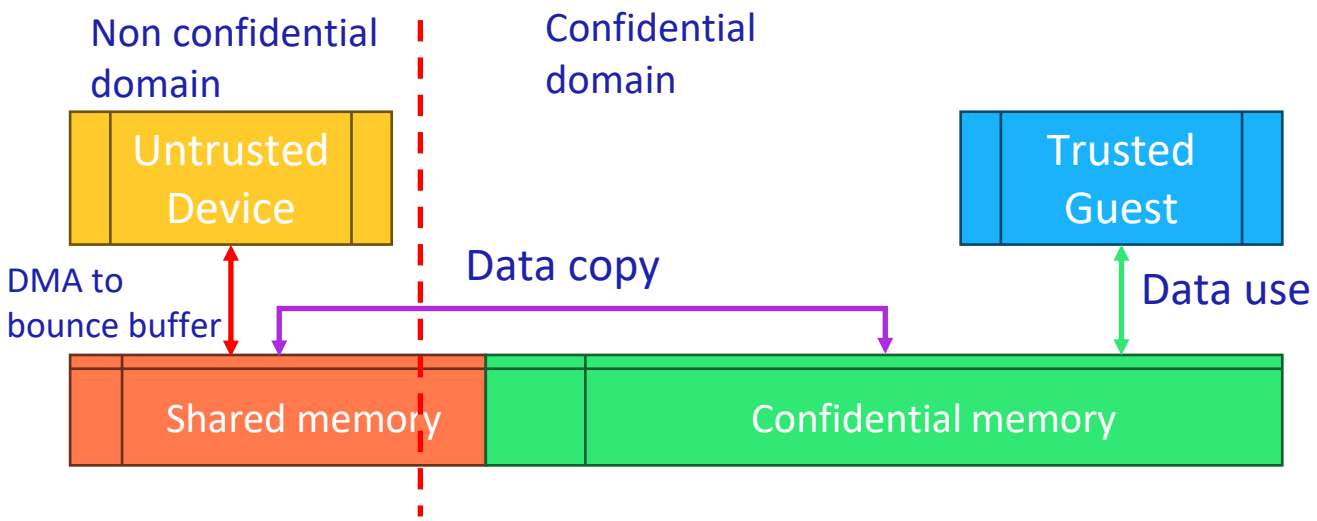
- **Изоляции физической памяти** на основе страниц и регионов на **M-уровне** .
- ПО домена супервизора **размещает** изолированные ВМ, приложения и даже вложенные гипервизоры **внутри домена**.
- **Менеджер** домена супервизора в каждом домене **изолирует** рабочие **нагрузки** с использованием **привилегированных режимов** ((V)U (V)S).
- **Изолированные домены** супервизора обеспечивают **гарантии конфиденциальности** и **целостности** данных/кода независимо от других доменов супервизора.

Confidential VM Ext компоненты



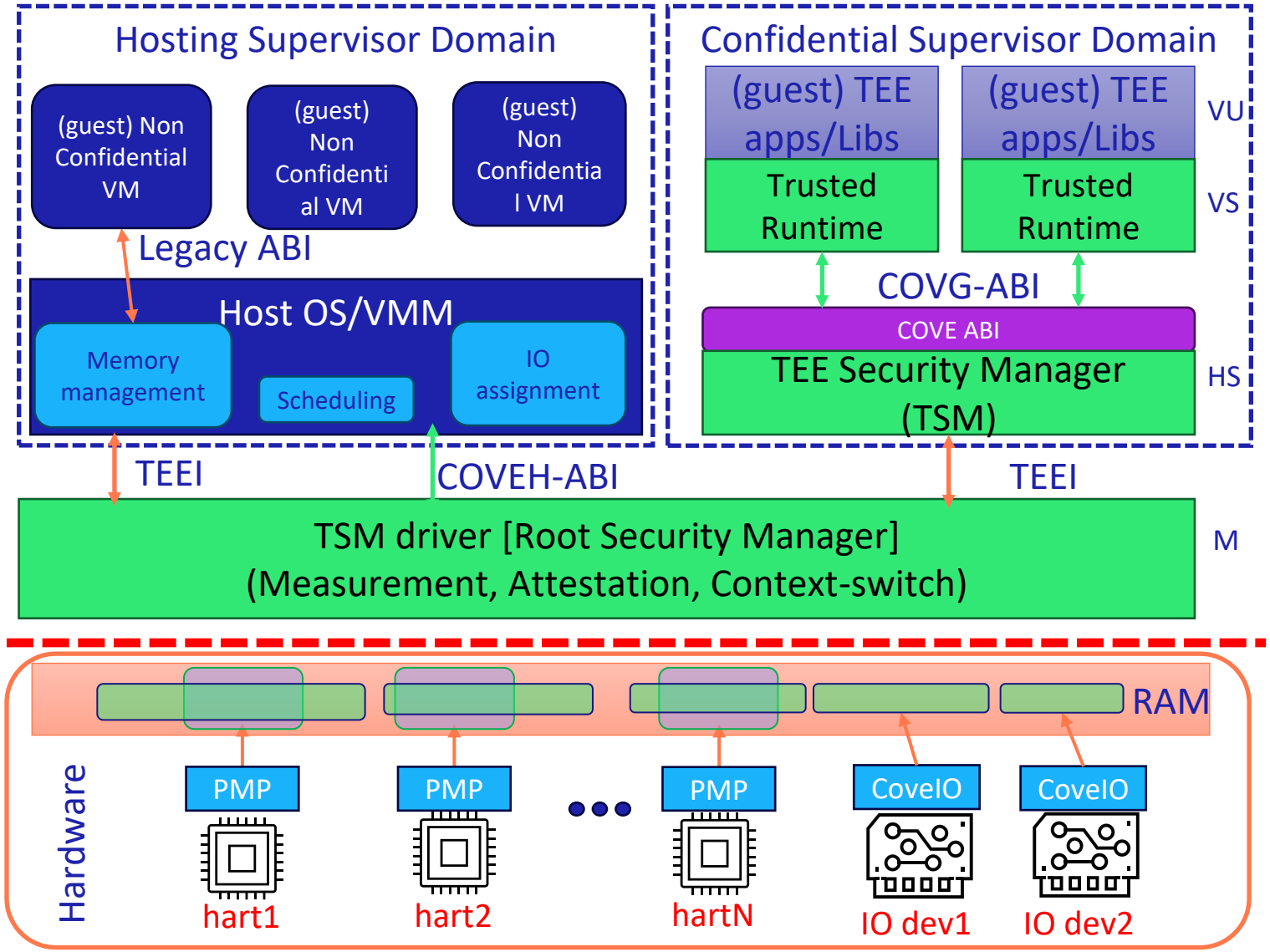
- TSM-driver предоставляет доступ к Trusted Execution Environment Interface (TEEI) – зависит от HW
- TEE Security Manager TSM - доверенный посредник между TEE и не-TEE нагрузками на одной платформе
- COVEH - управление жизненным циклом TVM: создание, добавление страниц в TVM, планирование выполнения TVM и т.д.
- COVEG - TVM запрашивает функции аттестации, функции управления памятью, общую память или пара-виртуализированный ввод-вывод.

CoVE I/O проблема



- Пара-виртуализированный ввод-вывод = многократное копирование данных через общую память с/на устройство ввода-вывода в/из конфиденциальной памяти.
- Буфер общей памяти требует дополнительной защиты канала передачи (например, шифрование данных на транспортном уровне).

CoVE IO предназначение



Установить **доверие** к устройству с помощью

- **идентификационных** данных устройства
- его **конфигурации** и состояния **безопасности**

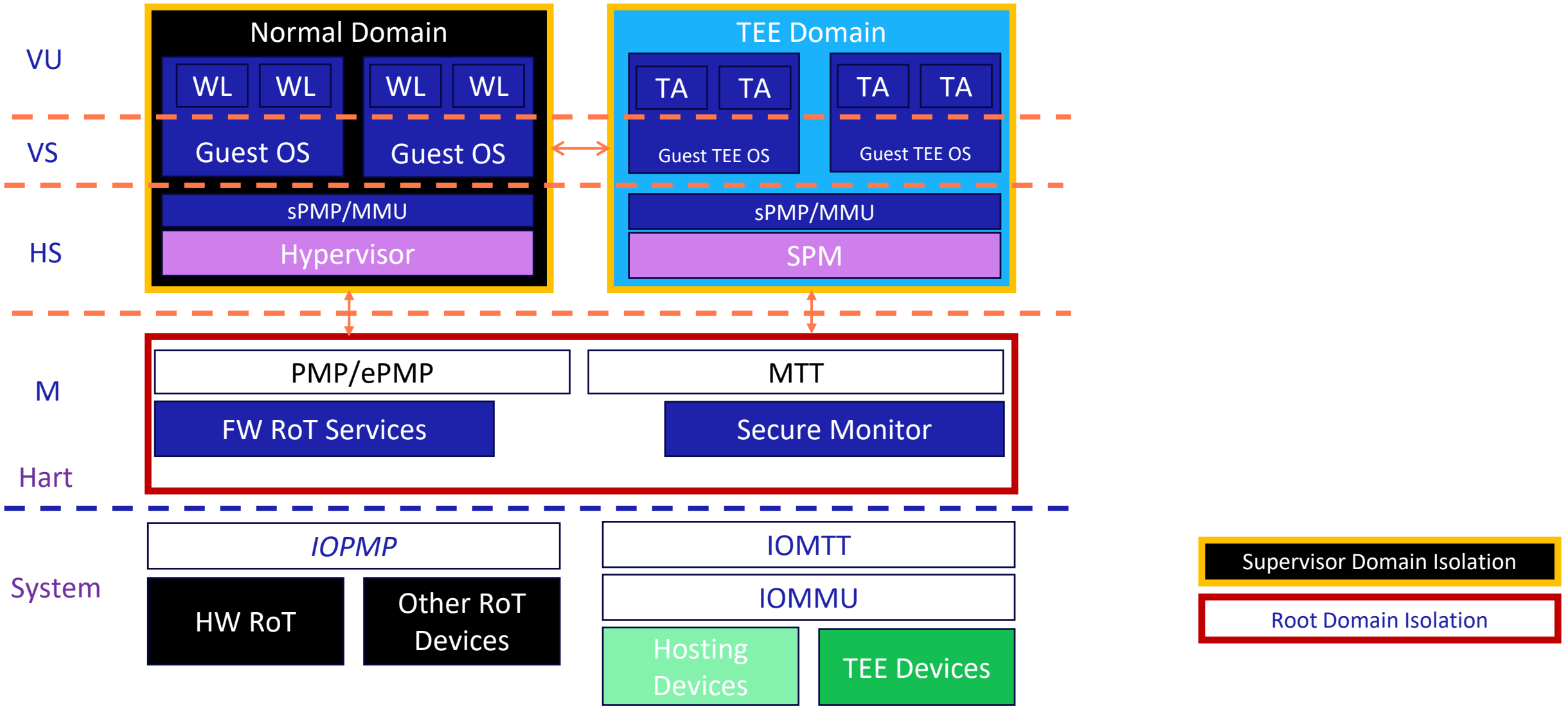
Гарантировать, что не доверенный компонент домена не сможет **перехватывать**, **изменять** или **контролировать** данные, передаваемые между **гостем** и назначенными ему **устройствами**.

Принимать устройства в TCB или нет, прежде чем разрешить им **прямой доступ** к **конфиденциальной** памяти и прежде чем иметь **возможность контролировать** и настраивать **устройства** ввода-вывода..

Заключение

- SmMTT –изоляция физического адресного пространства для более чем одного домена супервизора.
  - Несколько доменов - снижение размера общей TCB между доменами и аттестация каждого домена независимо от других доменов.
- CoVE – новый класс доверенной среды выполнения с аппаратной аттестацией - TVM.
  - TVM поддерживаются аппаратным, аттестуемым TCB, состояние выполнения и память изолированы от хостовой ОС/VMM и другого программного обеспечения платформы.
- CoVE IO –улучшает время работы внешних устройств с TVM не в ущерб свойствам конфиденциальности и защиты виртуальных машин.

Example with Virtualization



CoVE Example