



РусКрипто

XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Обзор аппаратных средств построения доверенной среды в системах на кристалле (СнК)

Колотников Алексей Владимирович

a.kolotnikov@ya.ru

|| Доверие между компонентами СнК строится на базе **изоляции** между **доверенной** и **общей** (богатой по разнообразию приложений) средой.

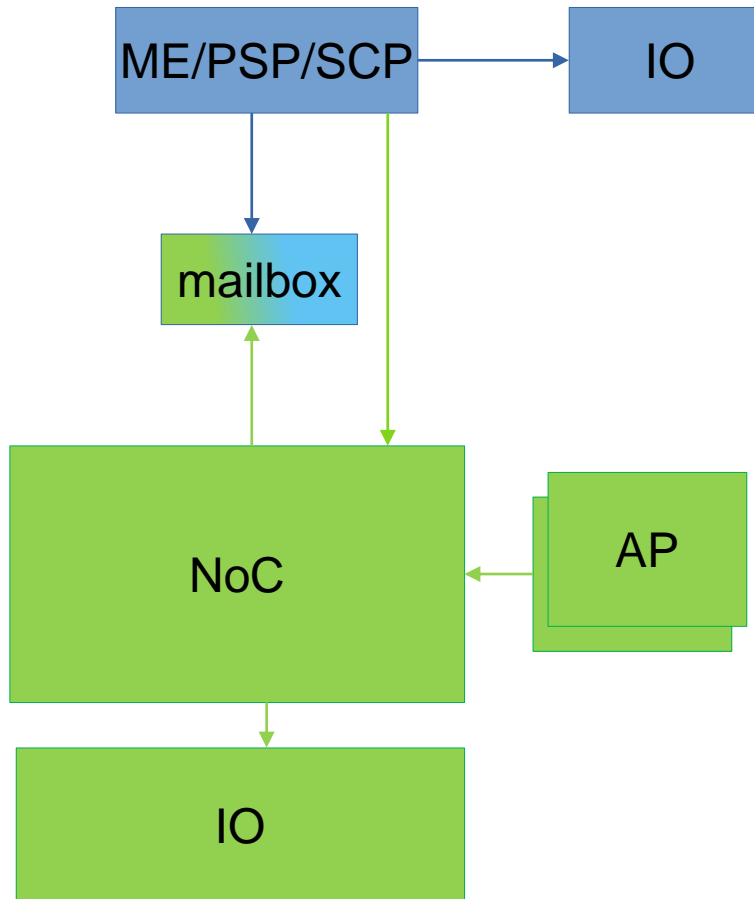
Такая изоляция может быть:

- физической
- временной
- криптографической
- логической

Далее рассмотрим каждый из способов чуть подробнее, с примерами.

Прим. такая систематизация может быть полезна для обоснования модели угроз и способов защиты в СнК.

Физическая изоляция



Это выделенная подсистема, которая продолжает работать параллельно с основной частью СнК с собственными ресурсами (память и IO). Доступ к этим ресурсам возможен только со стороны этой подсистемы.

Примеры: Intel ME(Management Engine(ARC/x86)), AMD PSP(Platform Security Processor (ARM Cortex A5)), ARM SCP/MCP (M7, A53, RISCv, etc.)

Проверка физически изолированной и маленькой (относительно всего СнК) подсистемы проще и может быть более детально проведена от архитектурного уровня, дизайна и до физического размещения на кристалле, если это предполагается ТЗ на СнК.

Примеры такой изоляции:

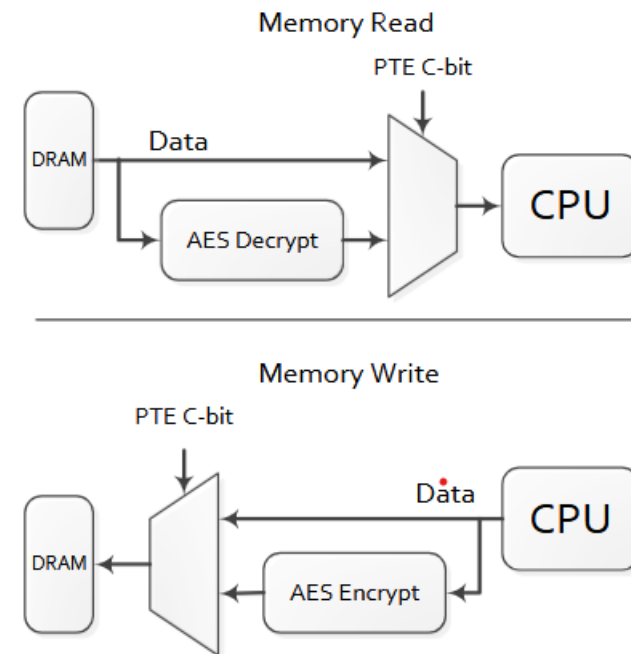
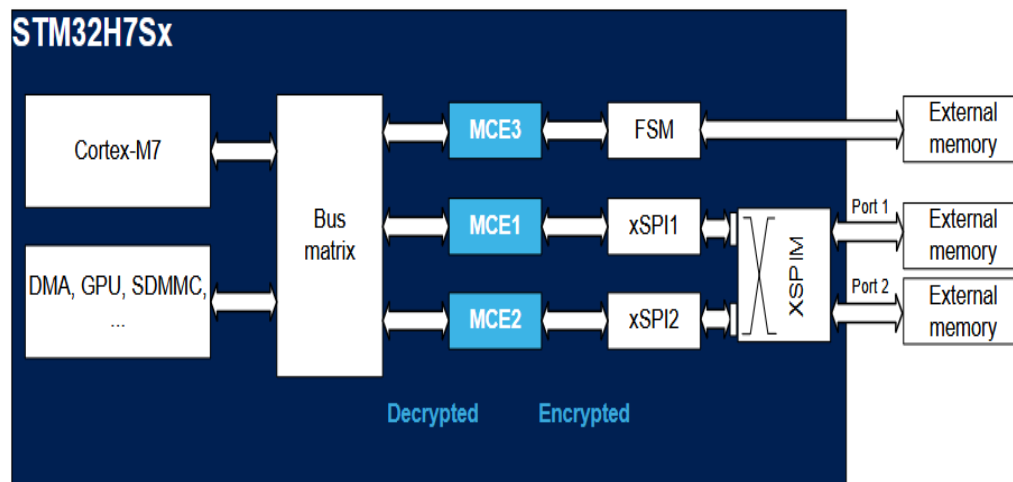
- отключение отладчика до следующего сброса СнК, если выбран режим загрузки пользователя, а не разработчика т.е. в этом сеансе работы отладчика не будет и включить его во время работы нет возможности предусмотренной в дизайне.
- блокировка (до следующего сброса) доступа к ОТР после некоторого этапа загрузки СнК
- обновление встроенного ПО только после перезагрузки

Этот способ изоляции тоже достаточно просто проверяется в модели, но более сложен для исследования на чипе т. к. отключаемые блоки могут быть распределены по СнК

Криптографическая изоляция

Часто СМК использует внешнюю память RAM, FLASH. Диапазоны адресов памяти могут быть предназначены для работы в разных режимах СМК и каждый диапазон может быть шифроваться на своем ключе.

Примеры: STM32 (MCE) Memory cipher engine, AMD Secure Memory Encryption (SME)



Логическая изоляция

Данный раздел не претендует на полноту описания т.к. каждый способ логической изоляции - это достаточно большая тема, сильно зависящая от выбранной архитектуры ядра (x86/RISCV/MIPS/ARM).

Ниже, основа логической изоляции для решений на архитектуре ARM v8.x/v9.x.

- User/kernel - EL0/EL1
- Виртуальная среда - EL1/EL2
- Trustzone - bit NS
- Контроль потока исполнения (ARM V9, lockstep)

Нужно отметить, что это самый широко используемый в больших СнК способ изоляции, но и самый трудный для проверки даже на модели т.к. здесь задействованы практически все подсистемы СнК.

Много программных решений базируются на корректной реализации логической изоляции. Это определено тем, что практически все ресурсы СнК (ядра, память, IO) могут логически переключаться между средами

ARM user/kernel - EL0/EL1

Это широко используемое разделение, идея которого базируется на контроле адресного пространства user из kernel.

Важные компоненты

- MMU в ядре
- Ряд специальных регистров ядра доступных только из EL1
- Механизм шлюза EL0->EL1 через инструкцию SYS
- SMMU для изоляции периферии

Для реализации этого требуется строить таблицы описания памяти и использовать специальные системные регистры ядра

Прим.: даже на этом уровне уже возникают проблемы побочного временного канала, известные как SPECTRA

ARM виртуальная среда EL2

Фактически это расширение kernel/user на VM/kernel т. е. идея такая же - контроль адресного пространства kernel из VM

Важные компоненты

- MMU в ядре
- Ряд специальных регистров ядра доступных только из EL2
- Механизм шлюза EL1->EL2 через инструкцию HMC
- SMMU для изоляции периферии

Для реализации этого также требуется строить таблицы описания памяти и использовать специальные системные регистры ядра.

ARM trustzone

Для поддержки такого режима работы придуман атрибут S/NS, (secure/non-secure) Этот атрибут присутствует практически во всех компонентах СнК

Важные компоненты

- Процессор поддерживает режим работы EL3 в котором доступны некоторые дополнительные системные регистры. Кроме этого есть режим EL1S/EL0S
- Протоколы AXI, CHI поддерживают передачу атрибута NS по СнК
- На входе в память находится фильтр(TZC), который разделяет память на зоны по атрибуту NS
- Кэш СнК разделяется по атрибуту NS
- Периферийные блоки могут быть фильтрованы по NS и если есть DMA, то надо выбрать атрибут NS для запроса
- MMU, SMMU транслируют атрибут NS согласно таблицам
- Механизм шлюза через инструкцию SMC

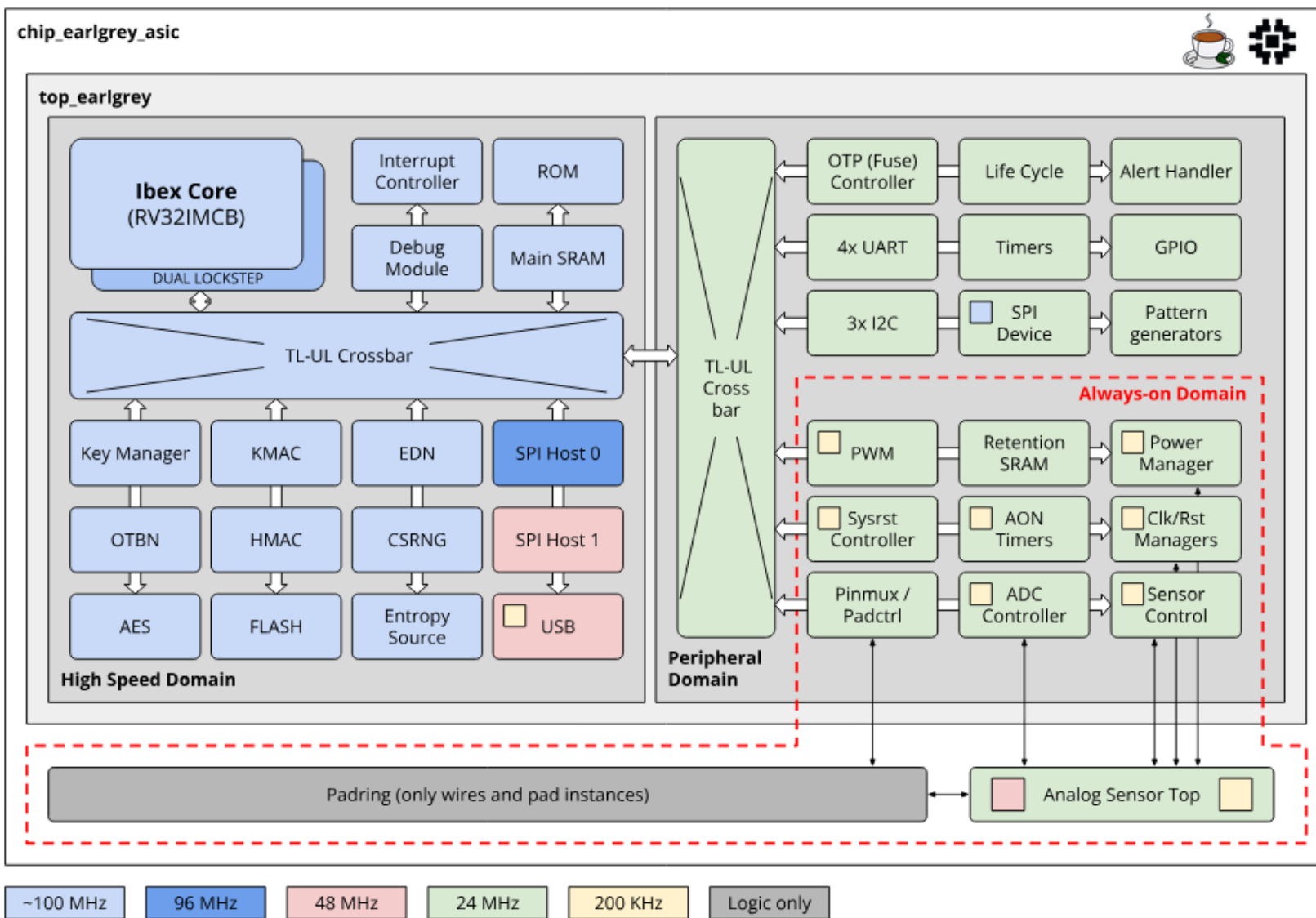
Выше перечислены некоторые(не все) компоненты для понимания того, что в СнК участвует в построении Trustzone и насколько это распределенная система

Поток исполнения программы может быть нарушен различными способами (от программных ошибок до аппаратных помех), тема достаточно обширная

Некоторые методы CFI(Control Flow Integrity):

- ECC
- Lockstep
- ARM PAC - Pointer Authentication
- ARM BTI - Branch Target Identification
- ARM MTE - Memory Tagging Extension

Что из средств защиты использовать в СнК?



OpenTitan Earl Grey

Критерии выбора средств защиты СнК

- ТЗ на безопасность СнК (что защищаем? какие могут быть атаки?)
- Размер проекта (процессор, микроконтроллер, спец. СнК)
- Доступные софт IP (что есть в дизайн студии и что можно купить)
- Выбранная технология (фабрика)
- Поставка фабричных IP (flash, OTP, DDK etc)

**Спасибо
за внимание!**



Вопросы?

Колотников Алексей Владимирович
a.kolotnikov@ya.ru