



RISC-V架构下OP-TEE 安全系统实践

桂兵 芯来科技

- **TEE 背景介绍**
- **Nuclei OP-TEE 方案**
- **Demo 展示**

TEE(Trusted Execution Environment):
由**GP**组织针对移动端设备，制定的安全解决方案。

现有**TEE**情况：

CPU 架构	支持TEE的硬件	支持TEE的软件
ARM	TrustZone	QTEE/TEEgris/ITrustee/ Trustonic/OP-TEE
RISC-V	PMP, Worldguard, IOPMP, AP-TEE	Keystone/PengLai/ MutilZone

RISC-V 没有GP TEE标准的开源软件方案

ARM Trustzone

- Processor Architecture
 - Monitor Mode
- System Architecture
 - AXI/AXI2AHB/AXI2APB
- Debug Architecture
 - Secure privileged/user invasive (JTAG)/non-invasive(Trace) debug
- Hardware Lib
 - TZASC/TZPC/GIC

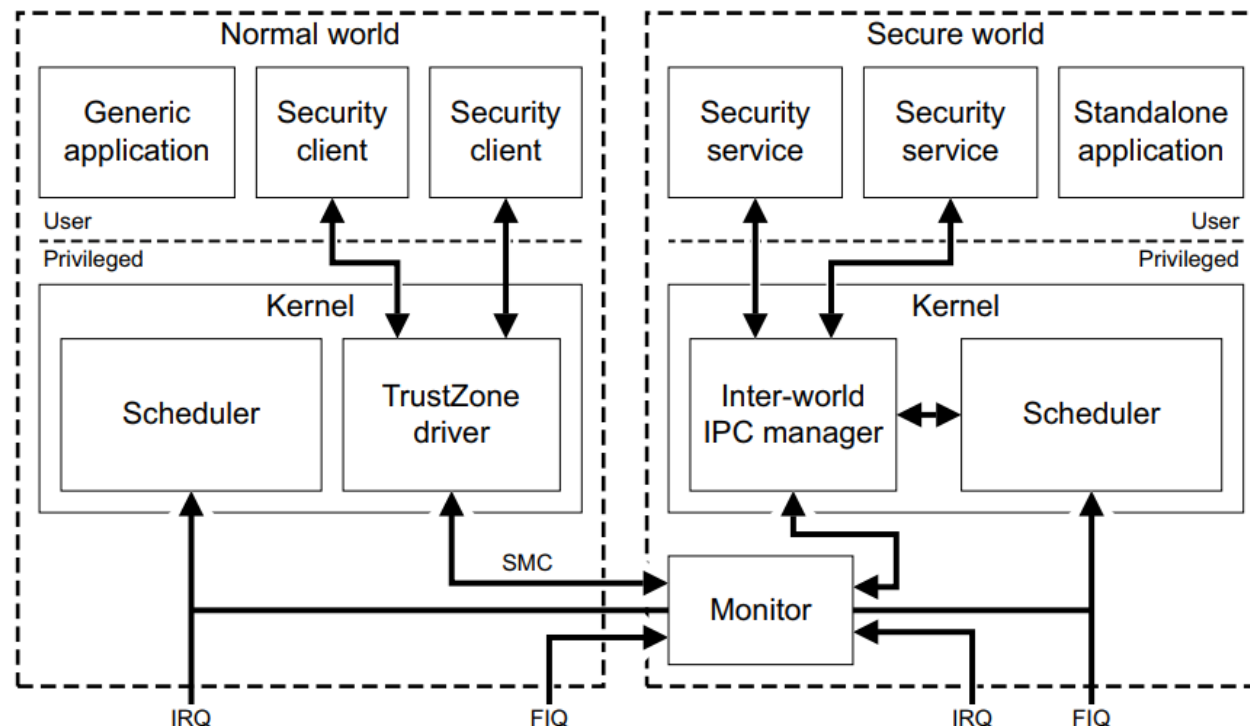


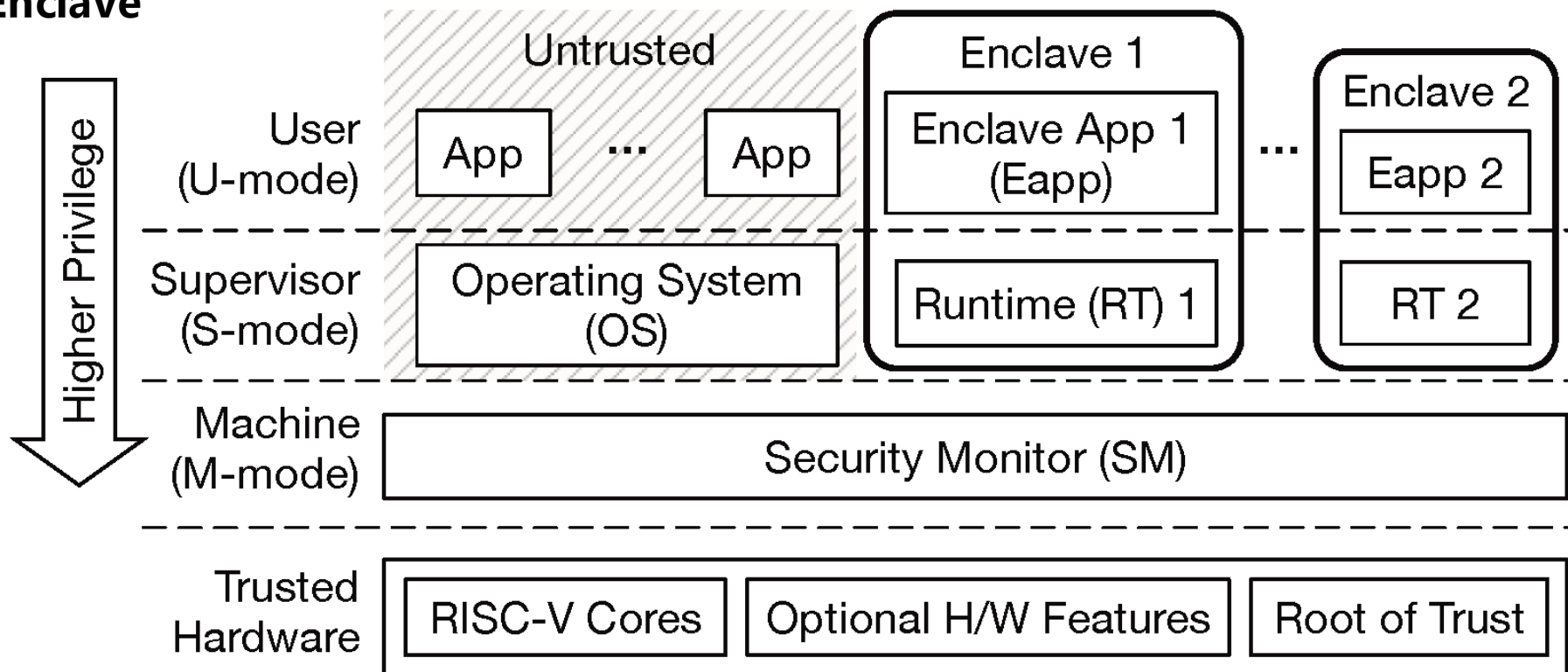
Figure 5-1 : A possible architecture with an independent Secure world OS

RISC-V

官方TEE标准: AP-TEE(in development)

Keystone Enclave

- PMP
- M/S/U



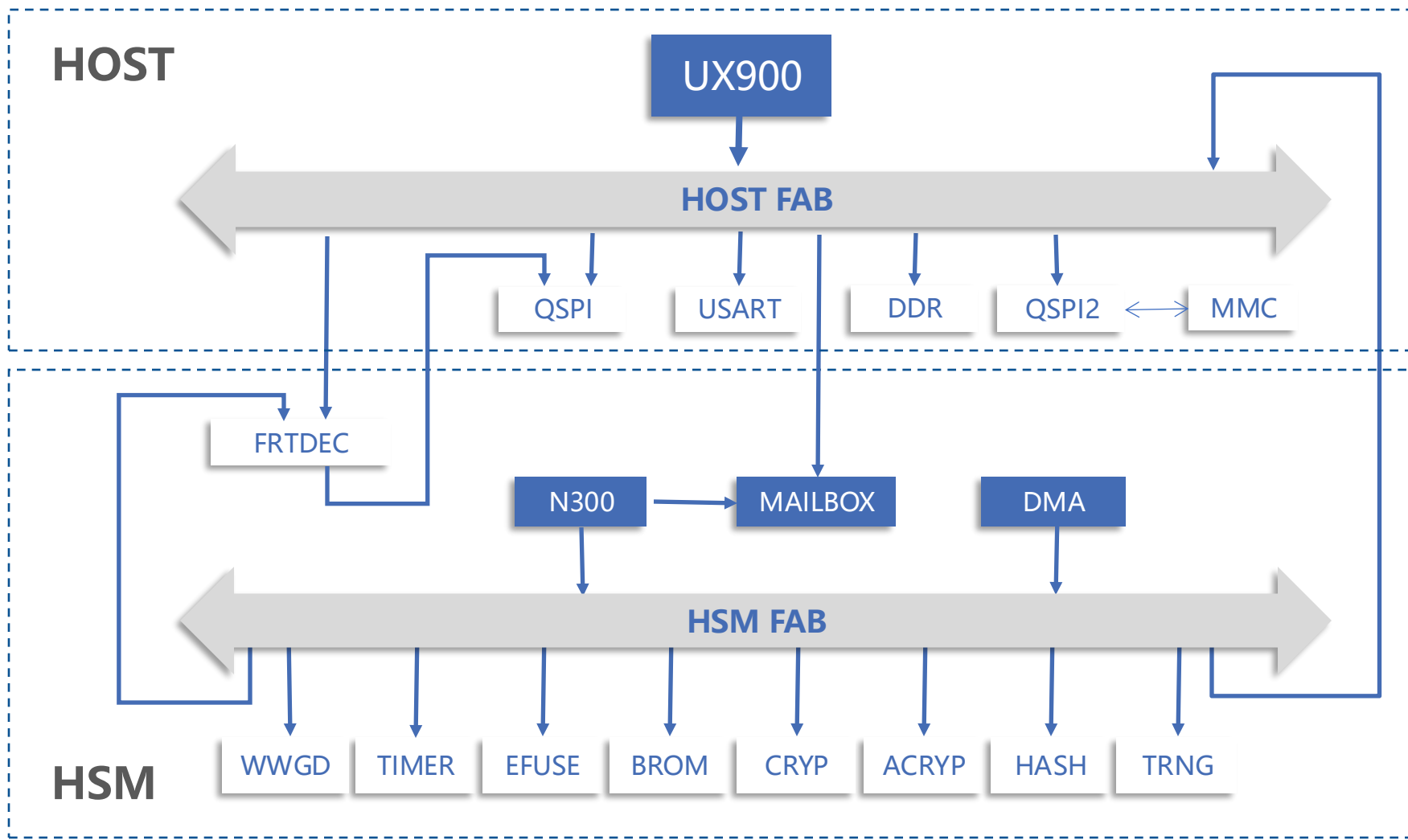
Nuclei OP-TEE 方案

HOST:

- UX900
- MMU/PMP/PLIC
- Nuclei Secure
 - hart/bus/cache/tlb with secure bit

HSM:

- N300
- BootROM
- Efuse
- Crypto



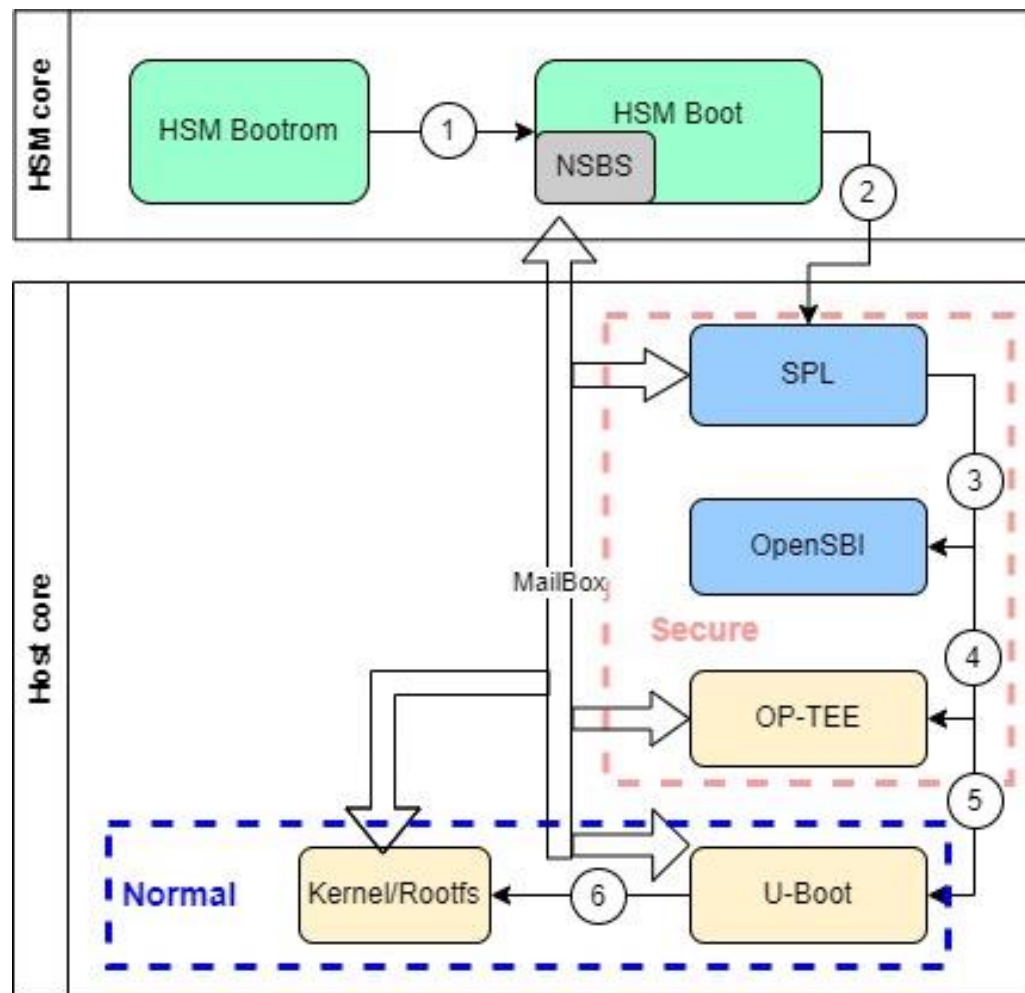
Nuclei OP-TEE 方案

安全启动

- HSM BootROM从flash加载hsmboot到HSM ILM, 验签解密
- HSM Boot从flash加载SPL到Host CLM, 验签解密, 运行NSBS等待Host请求crypto 服务
- SPL 初始化DDR, 从flash加载 opensbi/optee/uboot到DDR, 验签解密
- U-Boot从SD卡加载kernel/rootfs到DDR, 验签解密

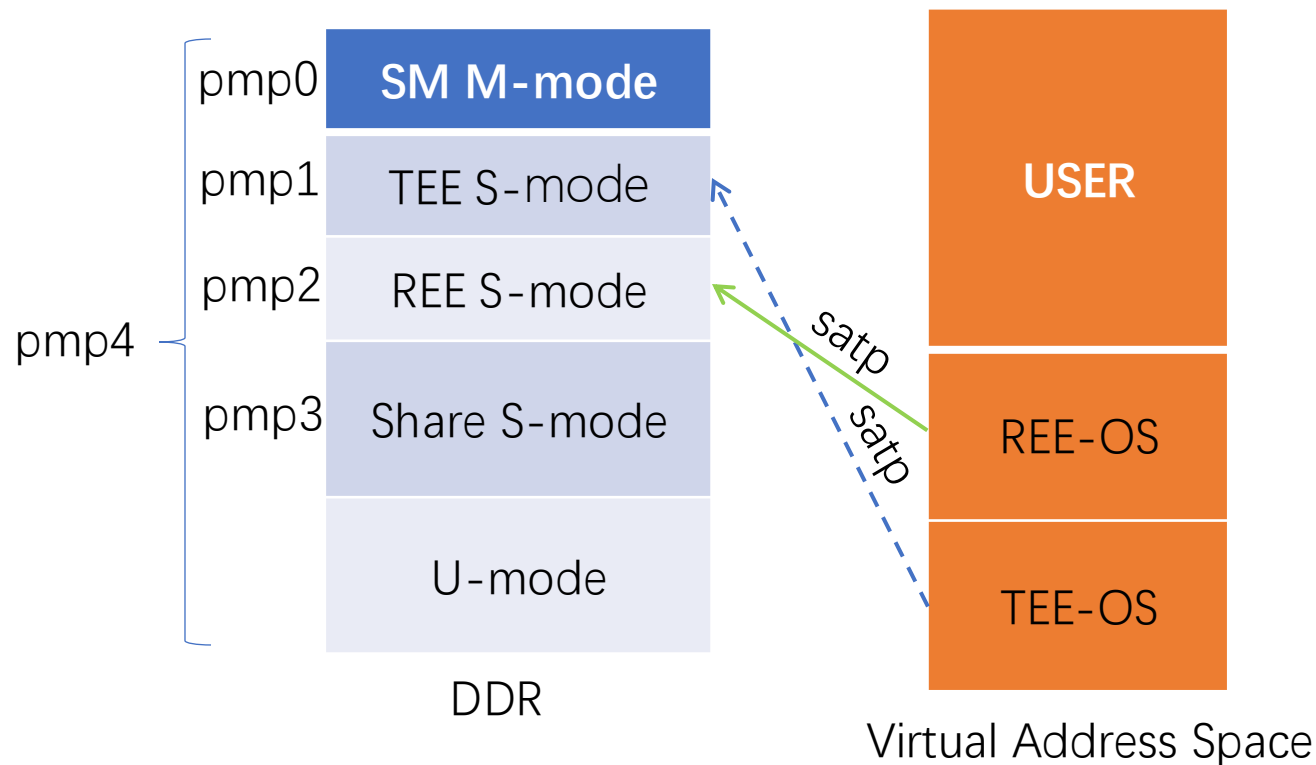
Host验签和解密, 通过MailBox请求HSM NSBS服务

- SPL->OpenSBI->OP-TEE
->U-Boot->Kernel



隔离机制-内存隔离，CPU安全状态隔离

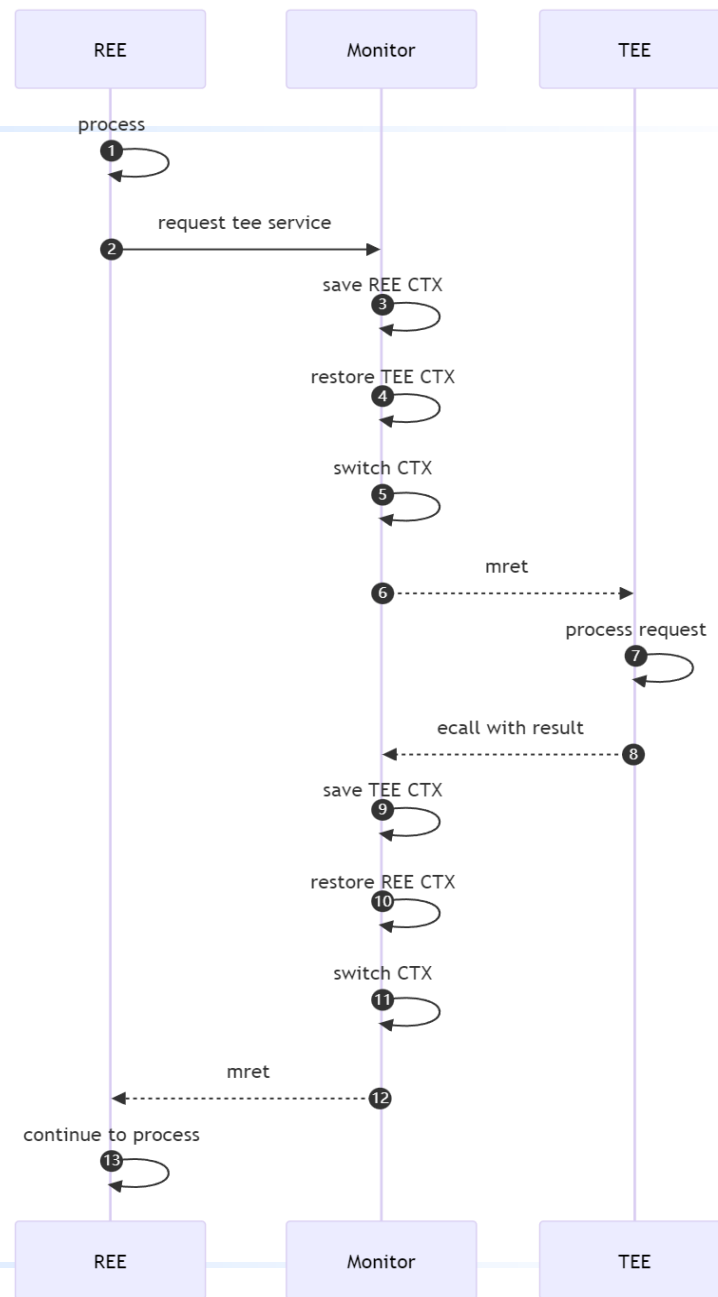
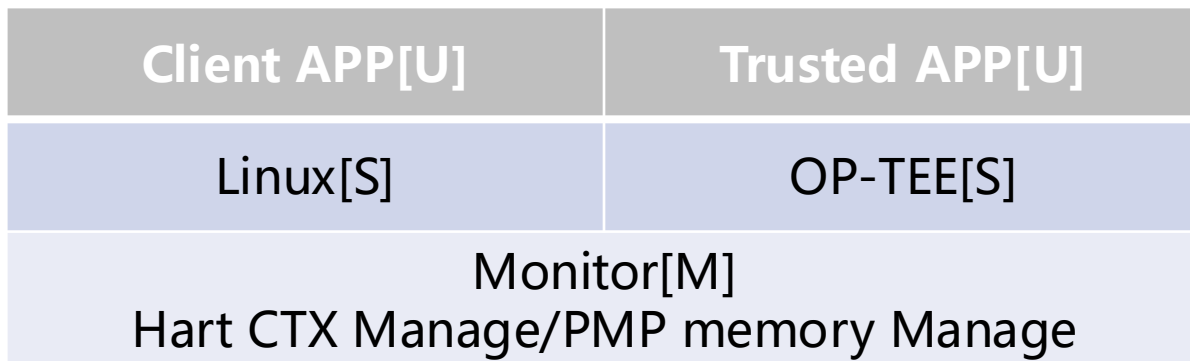
- PMP实现内存隔离：区分安全系统与非安全系统的内存地址空间
- M模式Monitor：管理CPU安全状态上下文，负责CPU安全状态上下文切换，执行地址空间切换
- PMP配置以编号小的优先级高
- 结合Nuclei Secure特性，CPU安全状态有硬件支持，BUS/Cache/TLB也区分硬件安全状态



Nuclei OP-TEE 方案

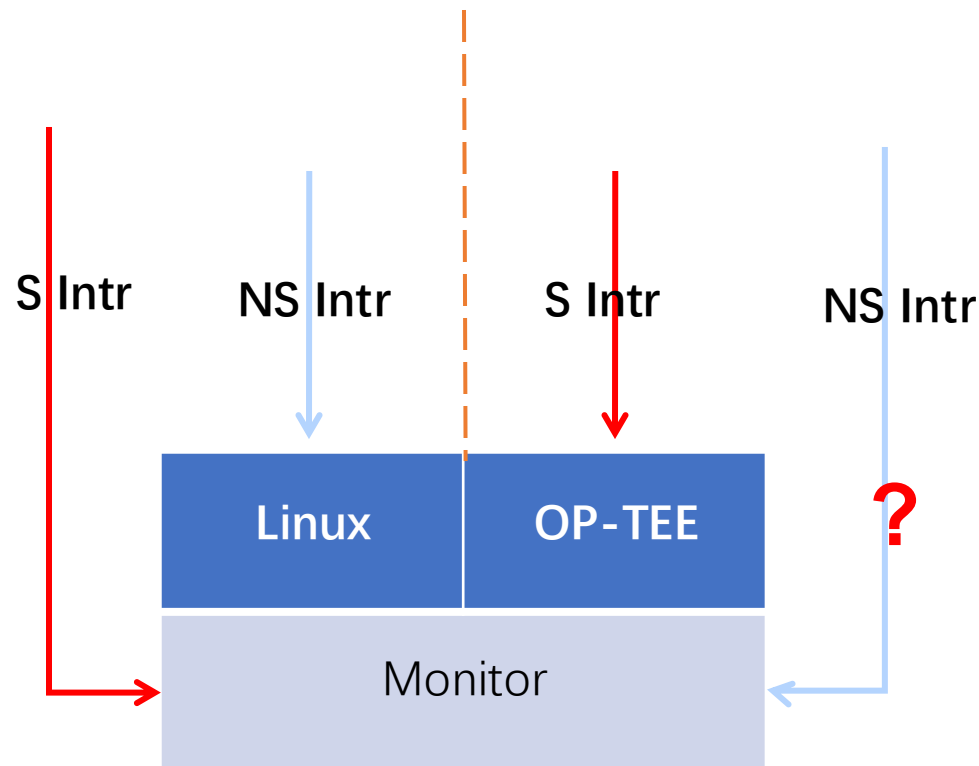
运行架构图及流程

- Monitor[M]: 管理安全状态上下文, 负责处理REE的请求, TEE的执行结果处理, 支持hart硬件安全状态
- REE-OS/TEE-OS[S]: 操作系统, 支持Cache安全, TLB安全
- CA/TA[U]: 用户程序



隔离机制-中断隔离

- 代理所有中断到S模式
- 对PLIC 中断使能模式分类：
 - M模式使能的中断：非本世界处理
 - S模式使能的中断：本世界处理
- Monitor 管理中断使能模式，比如进入非安全世界前，设置安全外设中断到M模式使能，非安全外设中断到S模式使能
- 为避免竞态，规定进入安全世界后，不响应非安全世界中断，但安全中断能打断非安全世界执行
- Nuclei PLIC硬件处理
 - M模式使能的中断，S模式不能修改中断相关寄存器
 - CPU在M模式下可修改PLIC 中断pending

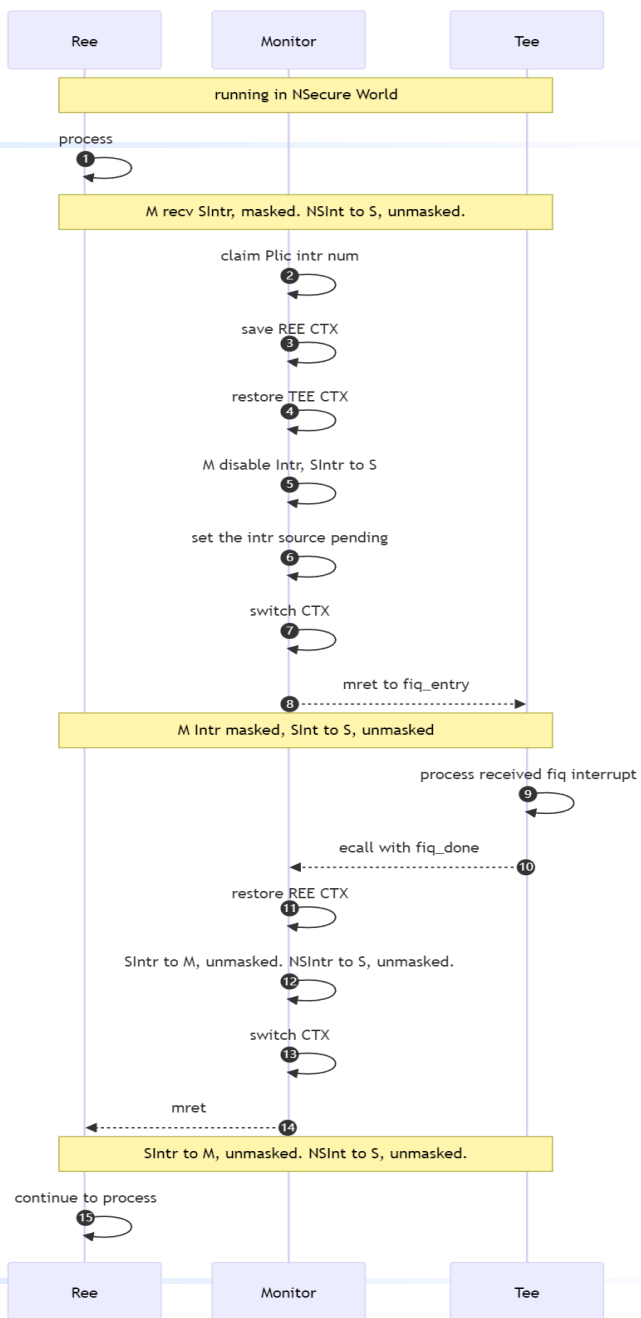


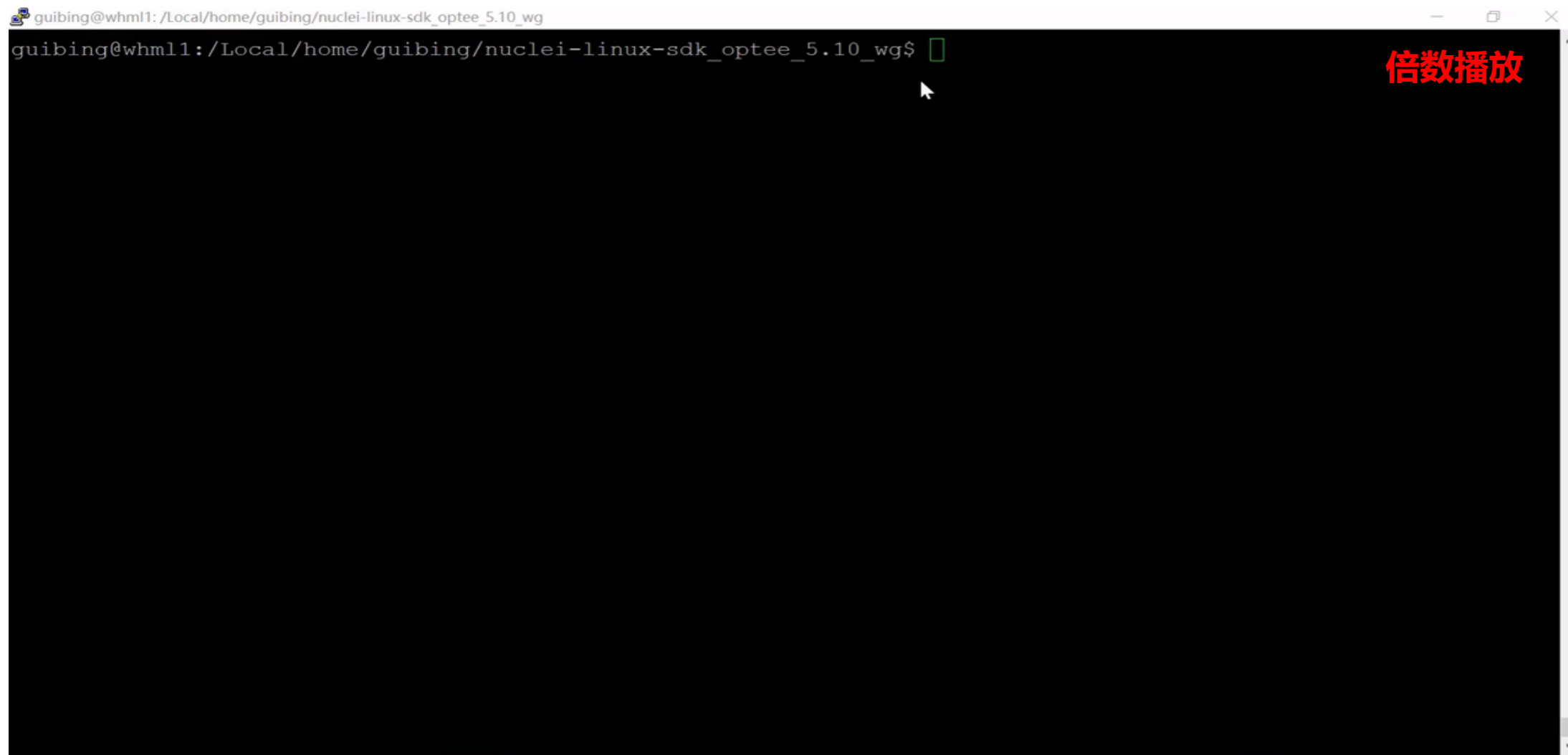
Nuclei OP-TEE 方案

中断处理举例

例子：安全中断打断非安全世界

- 获取中断号
- 保存REE执行上下文
- 恢复TEE执行上下文
- 关掉M模式中断使能，设置安全中断到S模式响应
- 设置中断源的pending
- 切换上下文，mret to TEE
- 恢复REE上下文
- 将安全中断的使能设置为M模式，非安全中断为S模式
- 切换上下文，mret to REE





A terminal window with a black background and white text. The title bar at the top reads "guibing@whml1: /Local/home/guibing/nuclei-linux-sdk_optee_5.10_wg". The terminal content shows a shell prompt "guibing@whml1: /Local/home/guibing/nuclei-linux-sdk_optee_5.10_wg\$" followed by a green cursor. A red text overlay "倍数播放" is positioned in the upper right area of the terminal window.

```
guibing@whml1: /Local/home/guibing/nuclei-linux-sdk_optee_5.10_wg$
```



THANK YOU