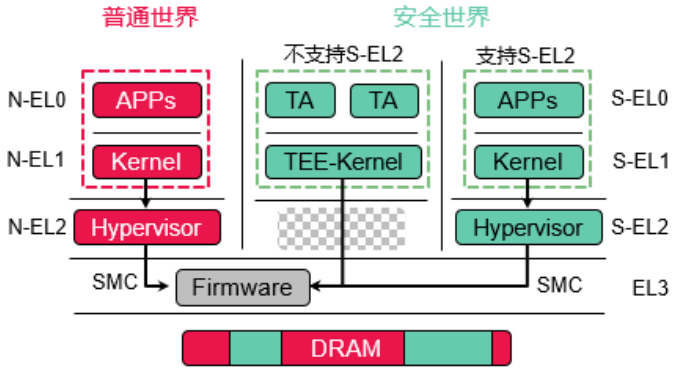
Lecture23 Confidential VM

其他机密虚拟化方案

ARM SEL2

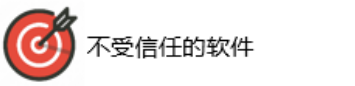
- **ARM TrustZone & Secure-EL2 (S-EL2)硬件扩展**
  - TrustZone: 与普通世界硬件隔离，被广泛应用于移动端
  - 从ARMv8.4开始引入的S-EL2扩展在TrustZone中支持了硬件虚拟化
    - S-EL2与普通世界的EL2功能相同



基于区域粒度的内存隔离
- 最多8个内存区域 (TZC-400)
- 可在EL3 & S-EL2进行配置

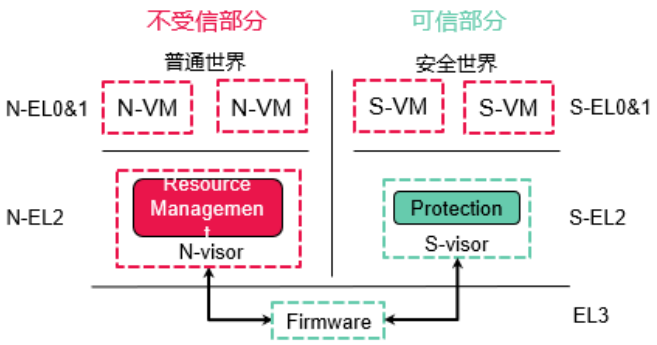
ARM TwinVisor

- **关键观察**
  - 在普通世界中已经存在功能成熟、被广泛应用的hypervisor了
- **将机密虚拟机的资源管理功能与保护机制解耦**



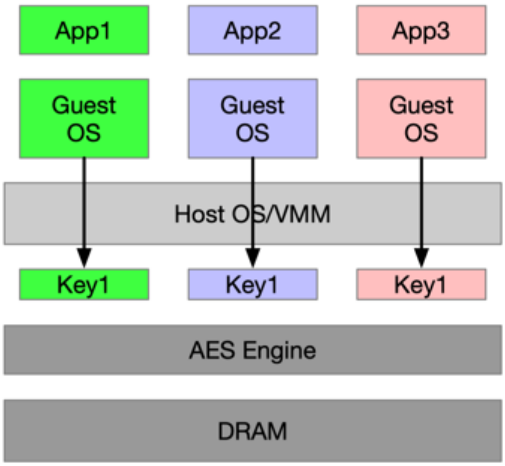
物理攻击、侧信道攻击、拒绝服务攻击

- 设备供应商需要提供硬件支持的attestation机制
- S-VMs需要保护自己的I/O数据安全



AMD Secure Encrypted Virtualization(SEV)

- **以虚拟机为粒度的Enclave**
  - 对不同的虚拟机进行加密
  - 每个虚拟机的密钥均不相同
  - Hypervisor有自己的密钥
- **安全模型的缺陷**
  - 依然部分依赖Hypervisor
    - 如：为VM设置正确的密钥



Intel Trusted Domain Extensions(TDX)

- **Intel TDX将VM（也称为TD）与虚拟机监控器和其他非TD软件隔离开**
  - Virtual Machine Extensions (VMX)
  - SEAM firmware
  - Multi-key, total memory-encryption (MKTME) technology