Google

Guestmem for pKVM

Fuad Tabba
tabba@google.com

Android Systems

Background Information

- Protected KVM on arm64: A technical deep dive
  - [Slides](), [Video]()
- pKVM code
  - [Android 14](), [Guestmem port]() (v13)
- Presentation on pKVM future use cases
  - [Trusted Applications in Protected VMs]()

android

The Armv8 Exception Model in Android (*Simplified*)

EL0	VMM	App	App	App
EL1	Host Kernel (Stage-1 Page Tables) - - - - - - - - - - - - - - - - - - - pKVM		Guest Kernel	
EL2	pKVM (Stage-2 Page Tables)			

android

Kernel: NOMAP
Guest S2: SHARED

Host mapcount = 0

share()

KVM_EXIT_HYPERCALL

host_fault()

Kernel: NOMAP
Guest S2: NOPAGE

Host mapcount = 0

Initial State

guest_fault()

Kernel: NOMAP
Guest S2: OWNED

Host mapcount = 0

Kernel: MAPPABLE
Guest S2: SHARED

Host mapcount = 0

host_fault()

host_unmap()

Kernel: MAPPABLE
Guest S2: SHARED

Host mapcount > 0

vcpu_run()

unshare();
KVM_EXIT_HYPERCALL

unshare();
KVM_EXIT_HYPERCALL

vcpu_run() && Userspace SHARED:
SMCCC_RET_ERR

Kernel: NOMAP
Guest S2: SHARED

Host mapcount = 0

host_unmap()

Kernel: NOMAP
Guest S2: SHARED

Host mapcount > 0

vcpu_run() && Userspace PRIVATE:
-EPERM

Guest Page Frame State (IPA)

Kernel: Guest frame memory attribute (*new, in an xarray*): {MAPPABLE, NOMAP}
Guest S2: Guest stage2 pkvm_page_state: {NOPAGE, OWNED, SHARED}

Host mapcount: page_mapcount() at host: = {0, > 0}