

KVM and Live Update

Extra topics

Paolo Bonzini & Sean Christopherson

KVM and Live Update

- Serialization format
- Sharing code with `kvm_*.ko`
- Confluence of pKVM and LUO?

Confluence of pKVM and LUO?

- “I have a beautiful patch, but it’s too small to fit this margin”
- Harder than it sounds
 - Page table management
 - Passing vmexit to untrusted hypervisor
- Hypothetical pKVM could act as caretaker, not vice versa without a lot of work

Serialization format

- To caretaker
 - Reconstruct VMCS/VMCB from scratch?
 - Reuse struct kvm_vcpu?
 - Reuse struct vcpu_{vmx,svm}?
- From caretaker
 - Serialize as ioctls

Code sharing

- Timer (VMX)
- HLT
- INVD
- WRMSR(ICR)
- WRMSR(deadline)

Code sharing

- WRMSR(kGSBASE, FSBASE, GSBASE, LSTAR, STAR)
- RDMSR
- CUID
- CR8 write
- WRMSR(PRED_CMD), RDTSC ?