Mid-term Homework

This homework assignment accounts for 10% of your final points.

Deadline: 2022.4.26 18:00

The file to be submitted for this assignment is:

1. report.pdf

Virtualization is the core technology that underlies many of today's IT infrastructures, including cloud computing and data centers. It leverages a software component, dubbed virtual machine monitor (VMM or hypervisor), together with some hardware support, to create an abstraction layer over computer hardware that enables the hardware resources of a single computer, including processors, memory, storage, etc., to be multiplexed by multiple virtual machines (VMs). VMs run their own operating systems (OS) and operate as if they are independent computers, though they are using only a portion of the underlying computer hardware. Virtualization enables more efficient utilization of physical computer hardware and secure isolation of computation on shared resources.

In this homework, you are about to find out how x86 (IA-32) and x86-64 virtualization technologies are designed and implemented, by reading some references by yourself and relating them to what you've learned in class. (RISC-V will have standard support to virtualization later, stay tuned). You are provided with documents related to Xen virtualization technology, an open-source virtual machine implementation that dominated Amazon AWS clouds, and Intel's CPU extension for supporting hardware-assisted virtualization. You can refer to these documents but go beyond them as you wish.

To help you organize your thoughts, you are asked to answer the following questions:

Note: answer the questions with your own words to avoid plagiarism!!! No points will be given to a question if a phrase of seven or more consecutive words are copied from the reference materials!!!

1. ## Terminologies of virtualization (20pts)

   (1) Define virtualization in 100 words? (2 pts)

   (2) Please explain the three usage models of virtualization: workload isolation, workload consolidation, workload migration. (6 pts)

   (3) List 3 well-known VMMs. (2 pts)

   (4) Explain the following terms: paravirtualization, full virtualization, binary translation, hardware-assisted virtualization, hybrid virtualization. (10 pts)

2. ## Privilege levels (25 pts)

   (1) How many privilege levels does x86 (IA-32) provide? How are they used by OS and user processes (considering an ordinary OS without virtualization)? Please provide three examples of the importance of privilege separation. (5 pts)

(2) What is ring compression? (3 pts)

(3) Without Intel VT-x, how does Xen address ring compression for X86 (IA-32)? (3 pts)

(4) Without Intel VT-x, how does Xen address ring compression for x86-64? (3 pts)

(5) What is ring aliasing? (3 pts)

(6) What are VMX root and VMX non-root in VT-x? (4 pts)

(7) How does Intel VT-x address the challenges of ring aliasing and ring compression? (4 pts)

3. ## System calls, interrupts and exceptions (28 pts)

(1) In the context of ordinary OS without virtualization, what are the purpose of system calls? What is the main difference between system calls and function calls? On x86-64 Linux, how are system call parameters passed to the kernel? (5 pts)

(2) What is a hypercall in Xen? (2 pts)

(3) How does Xen virtualize exceptions on x86 (IA-32)? What modifications does Xen make to the original x86 exception handlers? (4 pts)

(4) What are the challenges of virtualizing interrupts (especially regarding interrupt masking) on x86 (IA-32)? (3 pts)

(5) How does Xen virtualize interrupts on x86 (IA-32)? What is the benefit of such a design? (4 pts)

(6) What is VMCS in Intel VT-x? What are VM exits and VM entry? How are VMCS used during VM exits and VM entry (4 pts)

(7) How does Xen leverage Intel VT-x to virtualize interrupts? (3 pts)

(8) How does Intel VT-x support exception virtualization? (3 pts)

4. ## Address translation (27 pts)

(1) Explain x86 (IA-32) address translation. (3 pts)

(2) Explain x86-64 address translation (2 pts)

(3) Explain the relationship between guest virtual memory, guest physical memory, and machine memory. (3 pts)

(4) How does Xen manage the per-process page table in the VM and the per-OS page table in the VMM? (4 pts)

(5) What does “Address-space compression” mean? (3 pts)

(6) How does Xen address the problem of “Address-space compression”? (4 pts)

(7) What is Intel EPT? How to do MMU virtualization with Intel EPT? (5 pts)

(8) How does Xen allocate physical memory to each domain? (3 pts)

References

[1] Xen and the Art of Virtualization

[2] Xen 3.0 and the Art of Virtualization

[3] Extending Xen with Intel Virtualization Technology

[4] Intel Virtualization Technology

[5] https://sys.readthedocs.io/en/latest/doc/05_calling_system_calls.html

[6] https://pages.cs.wisc.edu/~remzi/OSTEP/vmm-intro.pdf

[7] Hybrid-Virtualization—Enhanced Virtualization for Linux

[8] Xen* Hypervisor Case Study - Designing Embedded Virtualized Intel® Architecture Platforms

[9] A Comparison of Software and Hardware Techniques for x86 Virtualization