Graduate Operating Systems

Spring 2023

1

Paper "Survey"

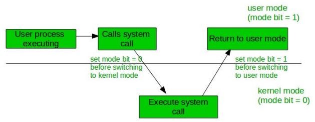
- Why simulating computer X on computer G?
- What if X = G, why is that useful?

- Virtual machine system, virtual machine (VM), virtual machine monitor (VMM)
- IBM example: security, reliability, development costs

2

Paper “Survey”

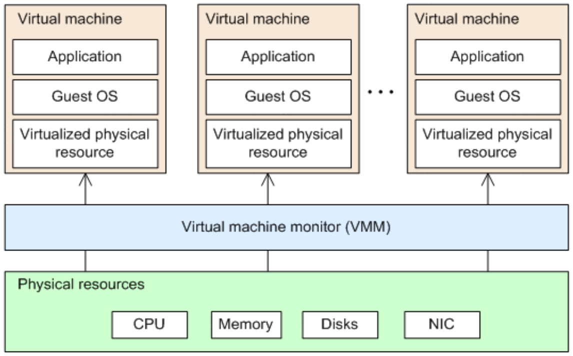
- Principles
  - Dual-mode systems



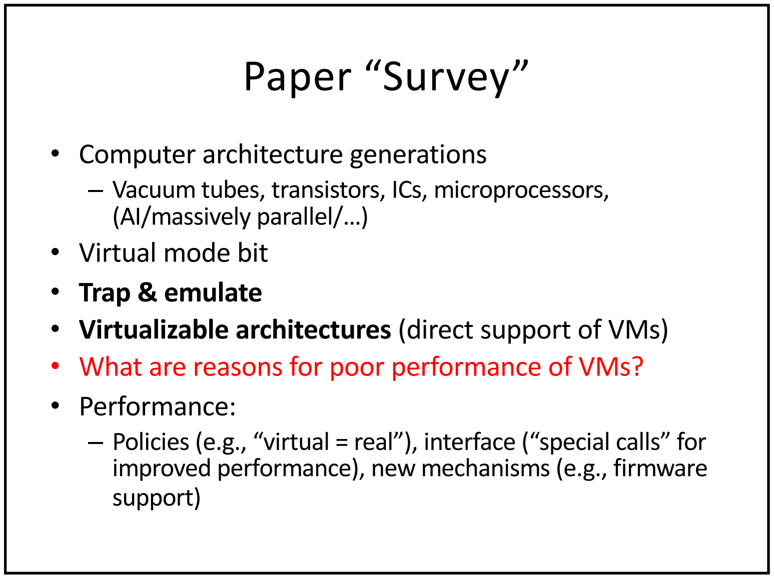
  - Figure 1: “single-kernel approach”
  - Figure 2: “multi-kernel approach”
  - Combination of **VM**, **Multiprogramming**, **Virtual Storage**

3

Paper “Survey”



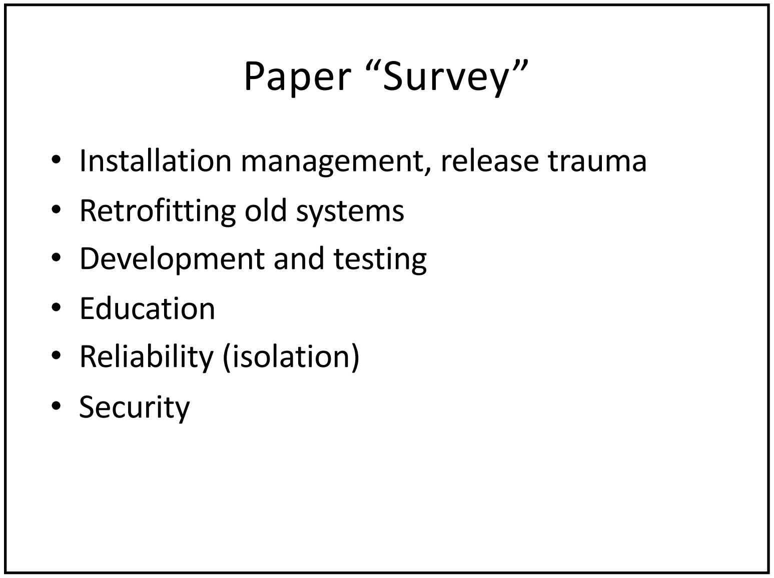
4



Paper “Survey”

- Computer architecture generations
  - Vacuum tubes, transistors, ICs, microprocessors, (AI/massively parallel/…)
- Virtual mode bit
- **Trap & emulate**
- **Virtualizable architectures** (direct support of VMs)
- What are reasons for poor performance of VMs?
- Performance:
  - Policies (e.g., “virtual = real”), interface (“special calls” for improved performance), new mechanisms (e.g., firmware support)

5



Paper “Survey”

- Installation management, release trauma
- Retrofitting old systems
- Development and testing
- Education
- Reliability (isolation)
- Security

6

Paper “VMM”

- Reasons for VM revival
  - Underused resources
  - Management overheads
  - Fragility, vulnerability
- “One app per machine” model
- Now: **hardware multiplexing**; **security** & **reliability**

- Encapsulation and migration
- Replication
- Suspend and resume
- Strong isolation

7

Paper “VMM”

- “Virtualizable”: direct execution supported (VM executing on real machine, while VMM has ultimate control of CPU); VM’s privileged and unprivileged code runs in CPU’s unprivileged mode (VMM runs in privileged)

- Sensitive instructions S
- Privileged instructions P
- **Virtualizable if S subset of P**

8

Paper “VMM”

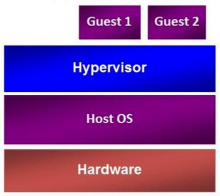
- Example of disabling interrupts
- X86: POPF, code segment register
- Paravirtualization
  - What is the biggest drawback?
- Direct execution + fast binary translation
  - Trace cache

Paper “VMM”

- Memory virtualization
  - Shadow page table
  - Balloon process
- I/O virtualization
  - Hosted architecture
  - Type 1 hypervisor

Paper “VMM”

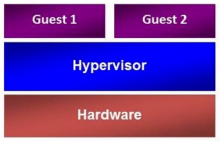
Type 2 Hypervisor



Examples:

- Virtual PC & Virtual Server
- VMware Workstation
- KVM

Type 1 Hypervisor

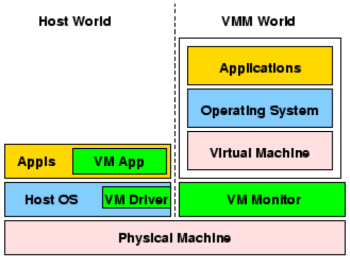


Examples:

- Hyper-V
- Xen
- VMware ESX

11

Paper “VMM”



12