Graduate Operating Systems

Fall 2018

Paper “Survey”

• Simulated computer X on computer G
• X = G, why?
• Virtual machine system, virtual machine (VM), virtual machine monitor (VMM)
• Security, reliability, development costs
• Dual-mode systems
• Combination of VM, Multiprogramming, Virtual Storage
Computer architecture generations
  – Vacuum tubes, transistors, ICs, microprocessors, (AI/massively parallel/…)

Virtual mode bit

Trap & emulate

Virtualizable architectures

Performance: policies, interface, new mechanisms
Paper “Survey”

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

Paper “VMM”

- Reasons for VM revival
- Less focus on multitasking, more focus on security and reliability
- Encapsulation and migration
- Replication
- Suspend and resume
- Strong isolation
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 \( P \)
• \textbf{Virtualizable if} \( S \) \textbf{subset of} \( P \)

Paper “VMM”

• Example of disabling interrupts
• X86: POPF, code segment register

• Paravirtualization
• Direct execution + fast binary translation
Paper “VMM”

- Memory virtualization
  - Shadow page table
  - Balloon process

- I/O virtualization
  - Hosted architecture
  - Type 1 hypervisor