Virtual Machines # 5.4  pg 315

Motivation

Security:
1. Security from malicious S/W and isolation
2. Failure & security & reliability of standard OS

Process context switch:
- triggered by timer interrupt
  1. save state of old process
  2. load state of new process - set timer
  3. give control to new process

Execution State
1) Registers e.g. PC
4) File descriptors (OS data structure)
3) TLB entries

Application S/W

H/W

Device driver

Kernel process

System S/W Components

Or provides notion of
process => dynamic entity
Program + execution state

Code + data

Process State - Registers
Other Motivation:
1. Managing S/w: allows different versions of S/w to run on same m/c
2. Managing H/w:
   - load balancing using migration
   - failure handling
     - either: migrate before failure
     - or: restart from last checkpoint

Virtualization through
1. Steaming Partitioning
2. Time Slicing
3. Emulation in S/w

Cost: context-switch overhead, TLB flush, cache pollution (increase in miss rate)
Problem 1 to Virtualization

VM:

VA → PA

(virtual address) → (physical address)

H/w

Problem 2 to Virtualization

ISA: (table on pg 340)

- Some instructions directly access VMM and execute via bypass
  - Some instructions may fail to execute
Para virtualization e.g. Xen → Open Source

- allows modification of guest OS

Read

Xen and the Art of Virtualization by P. Barham, et al. SOSP '93.

Support for VM in ISA (see pg 339)

- Intel VT-x
- AMD Pacifica
  - new execution modes for running VMs

1. Take Home Midterm Oct. 22 → Oct. 27
2. Project Proposal - Nov. 3 - 5%  
3. Project report (Midterm) - Nov. 17