Operating Systems Design (CS 423)

Elsa L Gunter

2112 SC, UIUC

http://www.cs.illinois.edu/class/cs423/

Based on slides by Roy Campbell, Sam King, and Andrew S Tanenbaum

3/12/11   1

Virtual Machines

- What is a Virtual Machine?
- An interface provided by software that is (or could be) the interface of actual hardware
- Examples?

3/17/11   2

Virtual Machine Monitor

- What is a Virtual Machine Monitor
- A layer of software that implements a Virtual Machine
- Examples?

3/17/11   3


Benefits of VMMs

- Industry: server consolidation
- Development: test machine consolidation
- Research
  - Run S/W at H/W level, below OS
  - Provides isolation where OS's don't
  - State encapsulation
    - Machine state -> VMM data structures; Disk -> File - These can be exported and examined
    - Encrypted disks
  - Portable services across OS's

3/17/11   4

Interfaces

- Standard system has H/W, OS, apps
- Both OS and apps run on top of H/W
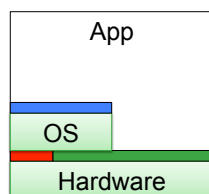
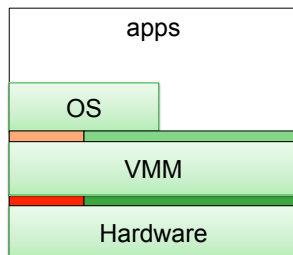3/18/11   5

Fixed Interfaces

- Advantages
  - H/W OS development can proceed independently
  - Components tend to be more portable
    - E.g. DOS apps still run on Vista w/ core 2 duo

- Disadvantages?

- Goal: All advantages with fewer disadvantages

3/17/11   6

Solution: new layer
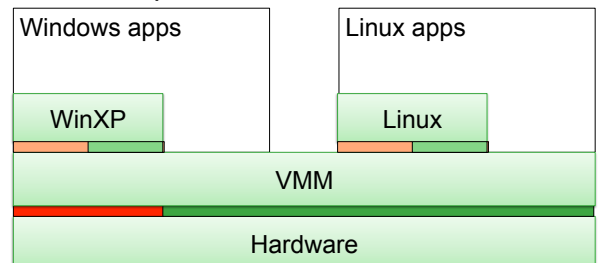
- Add new layer, called a VMM

```
          apps
    ┌──────────┐
    │    OS    │
    ├──────────┴───┐
    │     VMM      │
    ├──────────────┤
    │   Hardware   │
    └──────────────┘
```

VMM functions

- Translate one interface to another
- Run multiple virtual machines above

```
┌─────────────┐   ┌─────────────┐
│ Windows apps│   │ Linux apps  │
│ ┌─────────┐ │   │ ┌─────────┐ │
│ │  WinXP  │ │   │ │  Linux  │ │
├─┴─────────┴─┴───┴─┴─────────┴─┤
│            VMM                │
├───────────────────────────────┤
│          Hardware             │
└───────────────────────────────┘
```

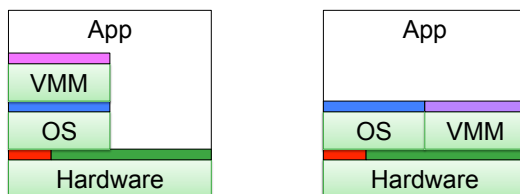## Smith and Nair

- ISA VMM
  - Both app and OS run above VMM
- ABI VMM
  - Only apps run above VMM
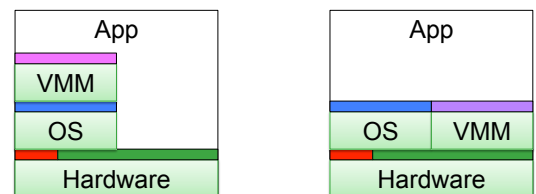 - VMM does not handle non-privileged instructions

```
┌──────────┐        ┌──────────┐
│   App    │        │   App    │
│ ┌──────┐ │        │          │
│ │ VMM  │ │        ├─────┬────┤
│ ├──────┤ │        │ OS  │VMM │
│ │ OS   │ │        ├─────┴────┤
│ ├──────┴─┤        ├──────────┤
│ │Hardware│        │ Hardware │
└─┴────────┘        └──────────┘
```

Smith and Nair

- Examples of ABI VMM?

```
┌──────────┐        ┌──────────┐
│   App    │        │   App    │
│ ┌──────┐ │        │          │
│ │ VMM  │ │        ├─────┬────┤
│ ├──────┤ │        │ OS  │VMM │
│ │ OS   │ │        ├─────┴────┤
│ ├──────┴─┤        ├──────────┤
│ │Hardware│        │ Hardware │
└─┴────────┘        └──────────┘
```

Questions

- This class we will focus on ISA VMMs
- Where do language-level VMMs fit?
- Where does VMWare fit?
- Where does Virtual PC for PPC fit?
- Other taxonomies also possible

Goldberg '74

- A virtual machine is…
- "an efficient, isolated, duplicate of the real machine"
- VM environment created by VMM
- Guest == virtual
  - Guest OS and apps run INSIDE a VM
  - Guest OS runs ABOVE a VMM
- Host == physical

VMM environment

- Duplicate
  - Virtual machine == physical machine
- Efficient
  - Runs almost as fast as real machine
- Isolated
  - VMM has control over resources
  - What are the resources the VMM controls?

3/17/11   13

VMM control and isolation

- Guest software can only access resources allocated to it

- VMM can reclaim resources

- E.g., More guest physical mem than phys mem

3/17/11   14

VMM research

- Record and replay
  - Debugging OSes
- Migration
  - Moka5 user convenience,
  - VMmotion for reliability
- Security
  - NSA NetTop
  - Isolated email and browser
  - Intrusion detection

3/17/11   15