Hey, You, Get Off of My Cloud

COS 316: Principles of Computer System Design

Amit Levy & Jennifer Rexford

Assignment 4 - Dopey Object Relational Mapper (DORM)

- Object relational mappers let programmers deal with high-level language types (objects, structs, etc) to interact with a SQL database
- Constrained to certain database schemata
  - Doesn’t support arbitrary databases
- Benefits
  - More convenient
  - Can abstract storage details (could also store structs in flat files, non-relational databases, etc)
  - Can allow enforcing high-level invariants in the programming language

Layering

- Network layering
  - Supporting various applications on top of various networks
- Cloud layering
  - Multiplexing resources at fine grained for many users
- Assignment 4 - layering abstractions in persistent storage
  - Translating a database query language to programming language constructs

Common themes that layering provides:

- Abstraction
- Separation of concerns
- ***Isolation***

Chinks in the Layering Armor

- Assignment 4: Abstractions can result in loss of
  - Expressiveness
  - Performance
  - Compatibility
- Today's lecture: Isolation is an asymmetric game
  - System builders must avoid breaking isolation at *every* layer
  - Attackers only need to find one chink in the armor

Hey, You, Get Off of My Cloud

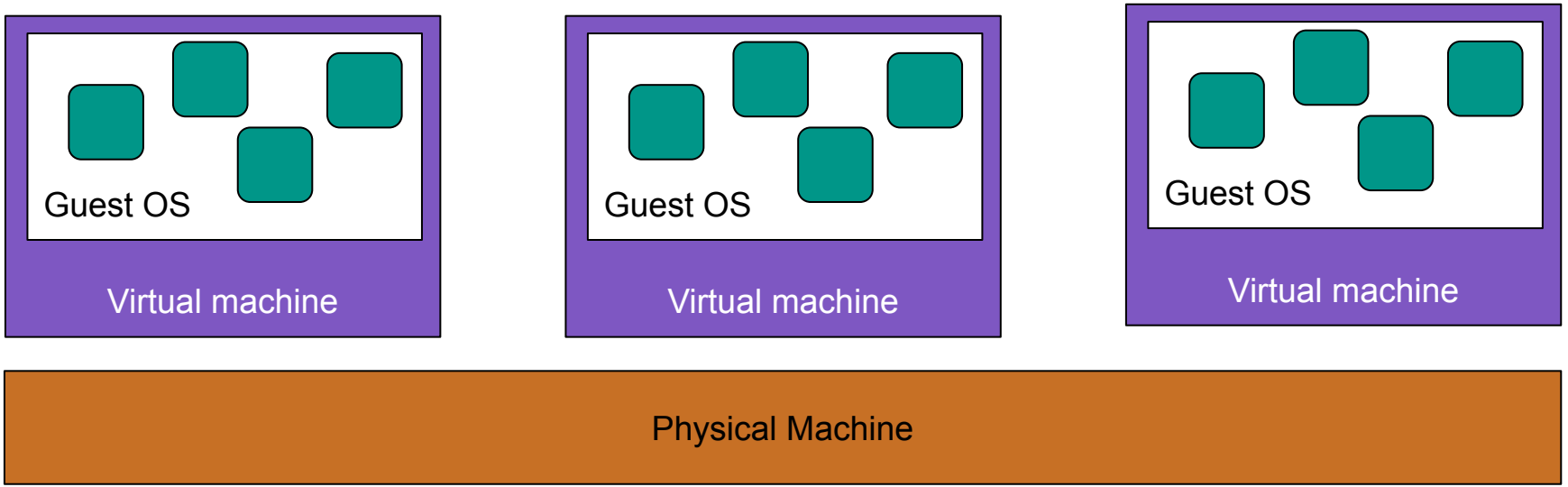
Hey, You, Get Off of My Cloud

- When: 2009
  - EC2 beta released 2006, full release 2008
  - Microsoft Azure, Rackspace Mosso, Google AppEngine, etc…

“Different EC2 instances *on* ***the same physical host*** are ***isolated*** from each other ***as though they are on separate physical hosts***” -EC2 Documentation

Is this true?

Virtual Machines



Virtualization

presents a physical machine as though many guest OSs had exclusive access

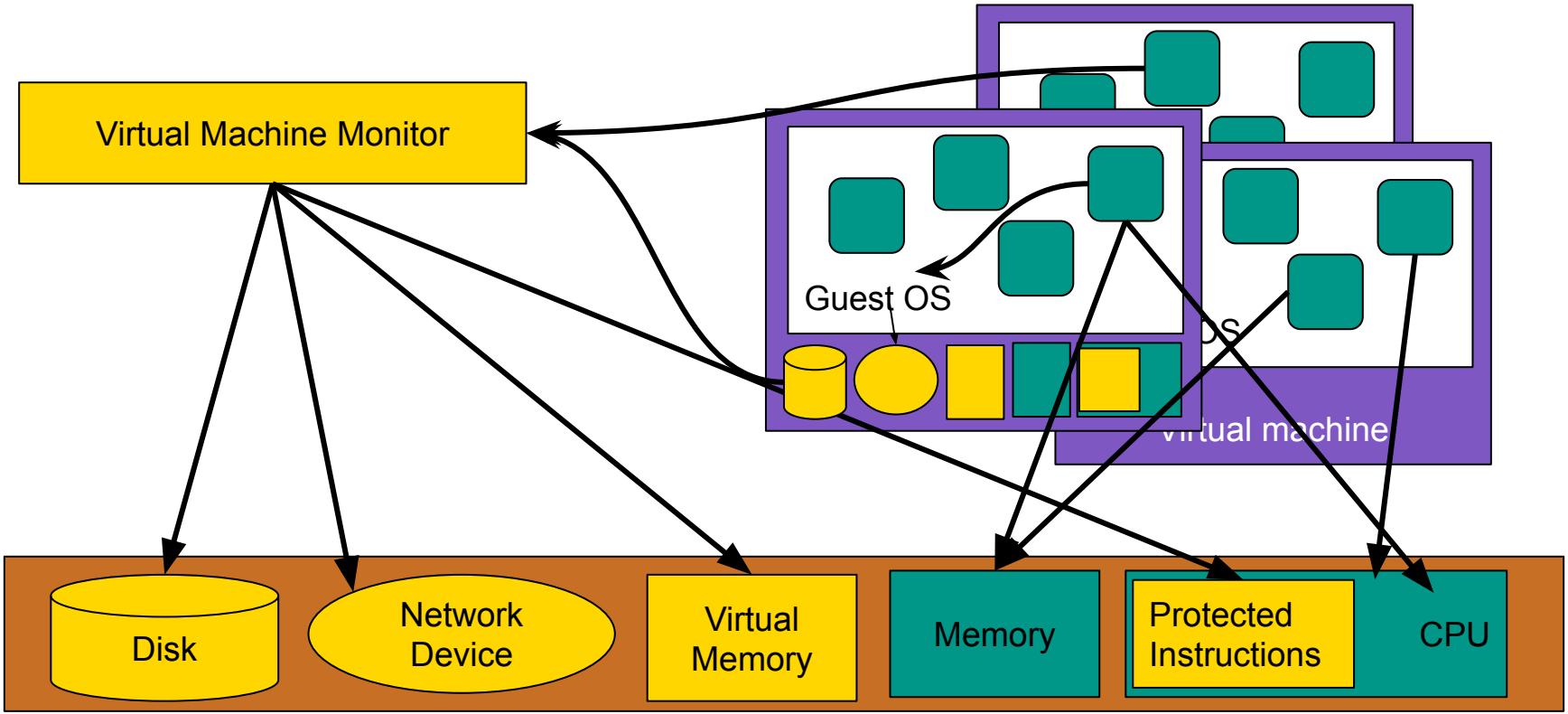
- Can VMs on the same host leak data to each other? ***Yes***
- Can an “attacker” place VMs on the same EC2 host? ***Yes***
- Can we fix this? ***No***

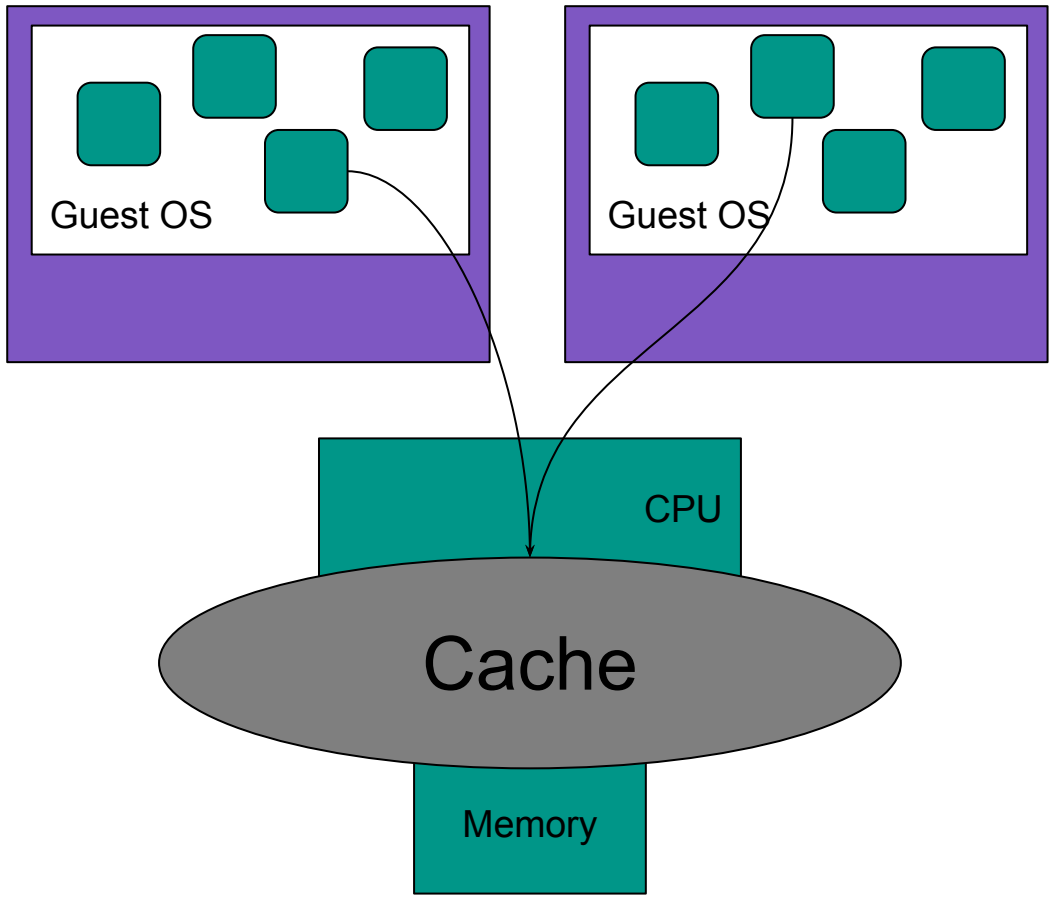
Can VMs leak information to each other?

Explicit channels vs Covert- & Side-Channels

- Explicit channels
  - Shared memory, shared files
  - Network stream, UNIX pipe
  - …
- Covert channels allow communication over mediums not designed for communication
- Side channels allow a component to use a covert channel to “attack” an unsuspecting “victim”
- Commonly
  - Metadata
  - ***Timing***

Virtual Machines




Guest OS
Guest OS
CPU
Cache
Memory

Prime and Probe

- **Prime:** read a large amount of data from memory to populate the CPU cache
- **Trigger:** wait until the other VM is scheduled
  - Wait until CPU cycle counter jumps by a large value
- **Probe:** measure the time it takes to read the memory again
  - If it takes a short time it is still in the cache
  - If it takes a long time, it's not

Meanwhile…

```
if some_secret == true then
  read_large_data_from_memory()
else while(True)
```

Placing VMs on The Same Host

- Key observation: Cloud providers want to pack VMs on few hosts
  - E.g., can power off unused machines
- If we provision VMs close in time, we'll probably get lucky
- How do we check? Network probing
  - Ping times
  - IP address allocation
  - Hardware MAC addresses
  - Hardware fingerprinting
  - …

- Can VMs on the same host leak data to each other? ***Yes***
- Can an “attacker” place VMs on the same EC2 host? ***Yes***
- Can we fix this? ***No***