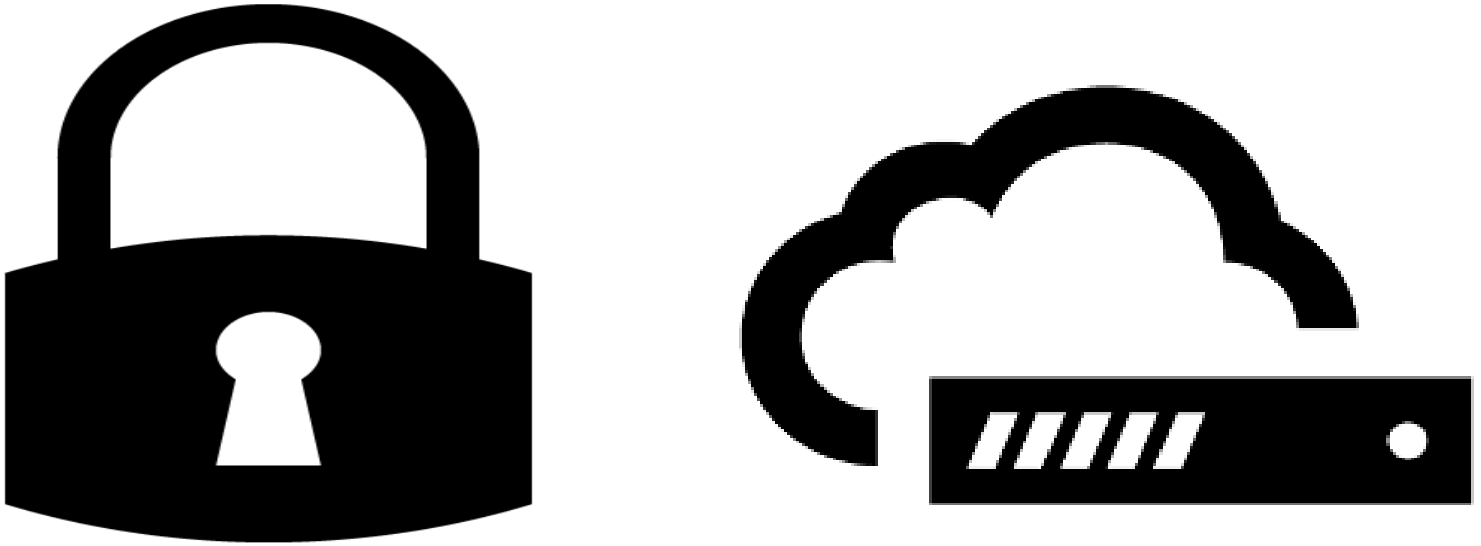
# Securing your Virtual Datacenter



Part 1: Preventing, Mitigating Privilege Escalation

NSRC

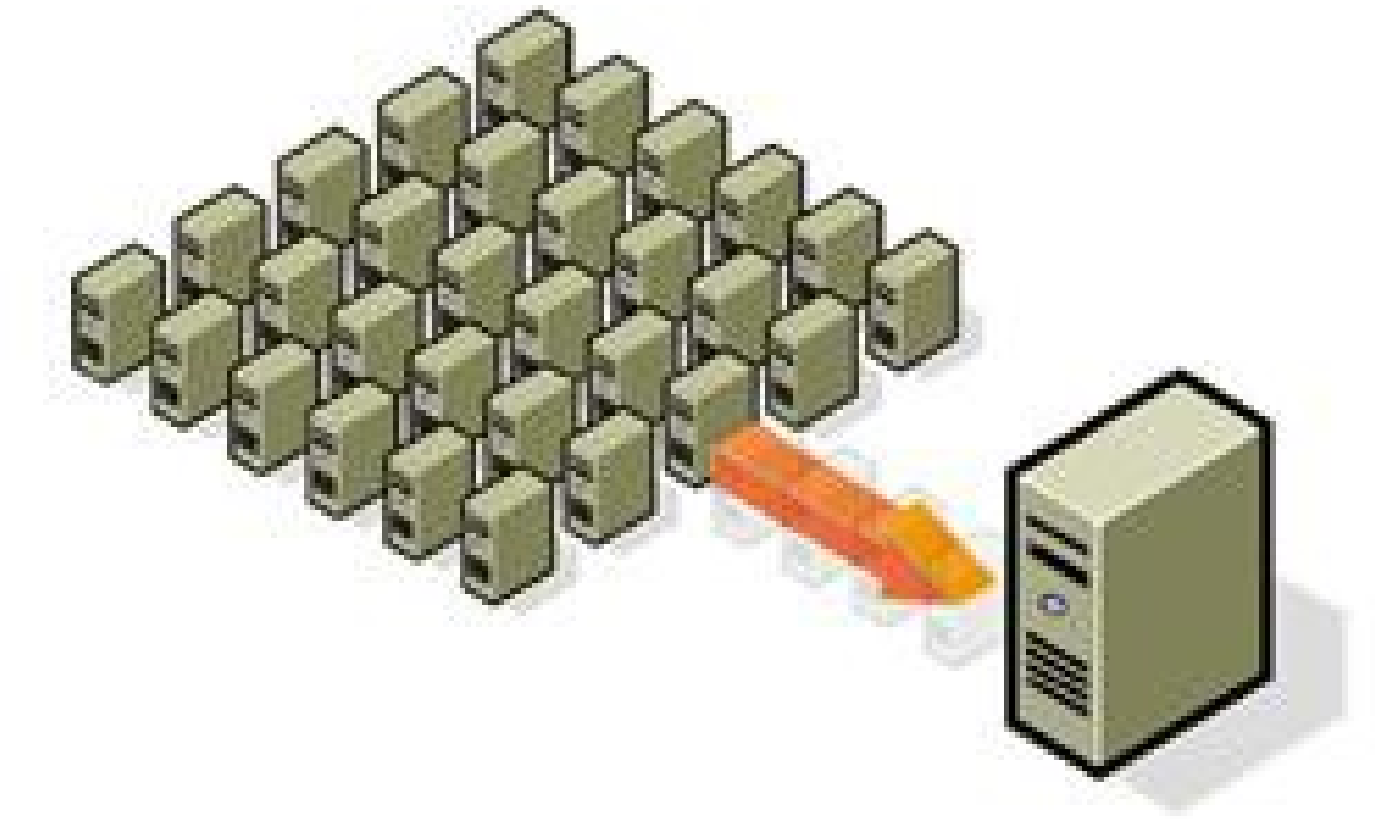
Network Startup Resource Center

UNIVERSITY OF OREGON

# Before We Start...

- Today's discussion is by no means an exhaustive discussion of the security implications of virtualization
- Recommendations for securing infrastructure may or may not fit in your environment
- If you have any questions  there may be time after the talk, otherwise, please feel free to approach me after

# Virtualization?



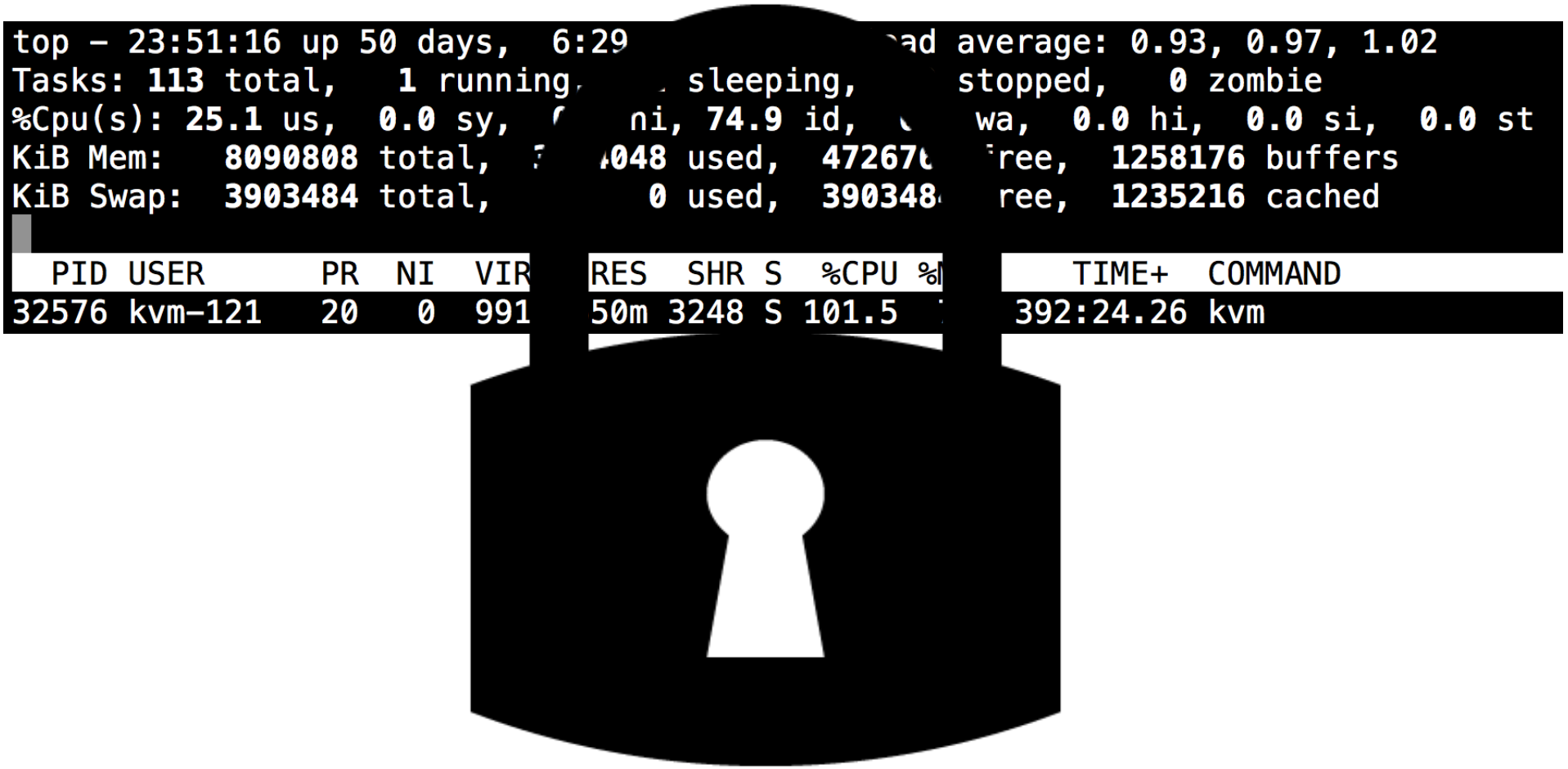
# Why?

- Consolidation
  - Most systems are under-utilized, especially the CPU is idle for much of the time
  - Do more work with less hardware
  - Reduced space and power requirements
- Management
  - Snapshot/restore, cloning, migration
  - Increased isolation between services

# Servers...

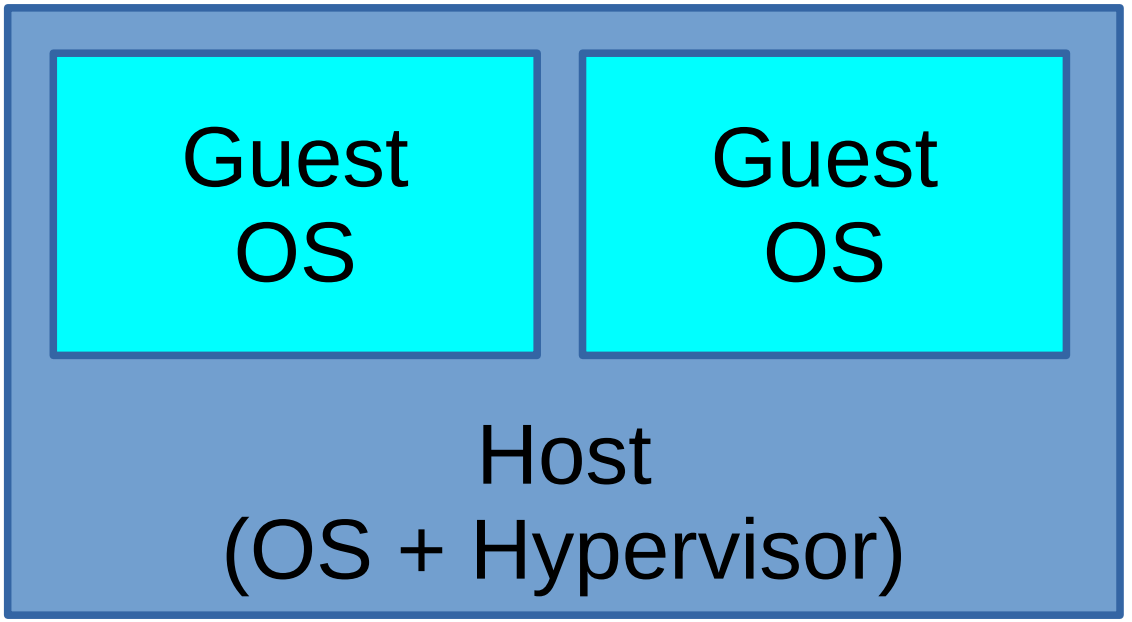
# Servers.

# Where does the lock go?



# Terminology

- The host is the physical machine running the virtual machine
- The guest is the emulated (virtual) machine
- One host could be running many guests



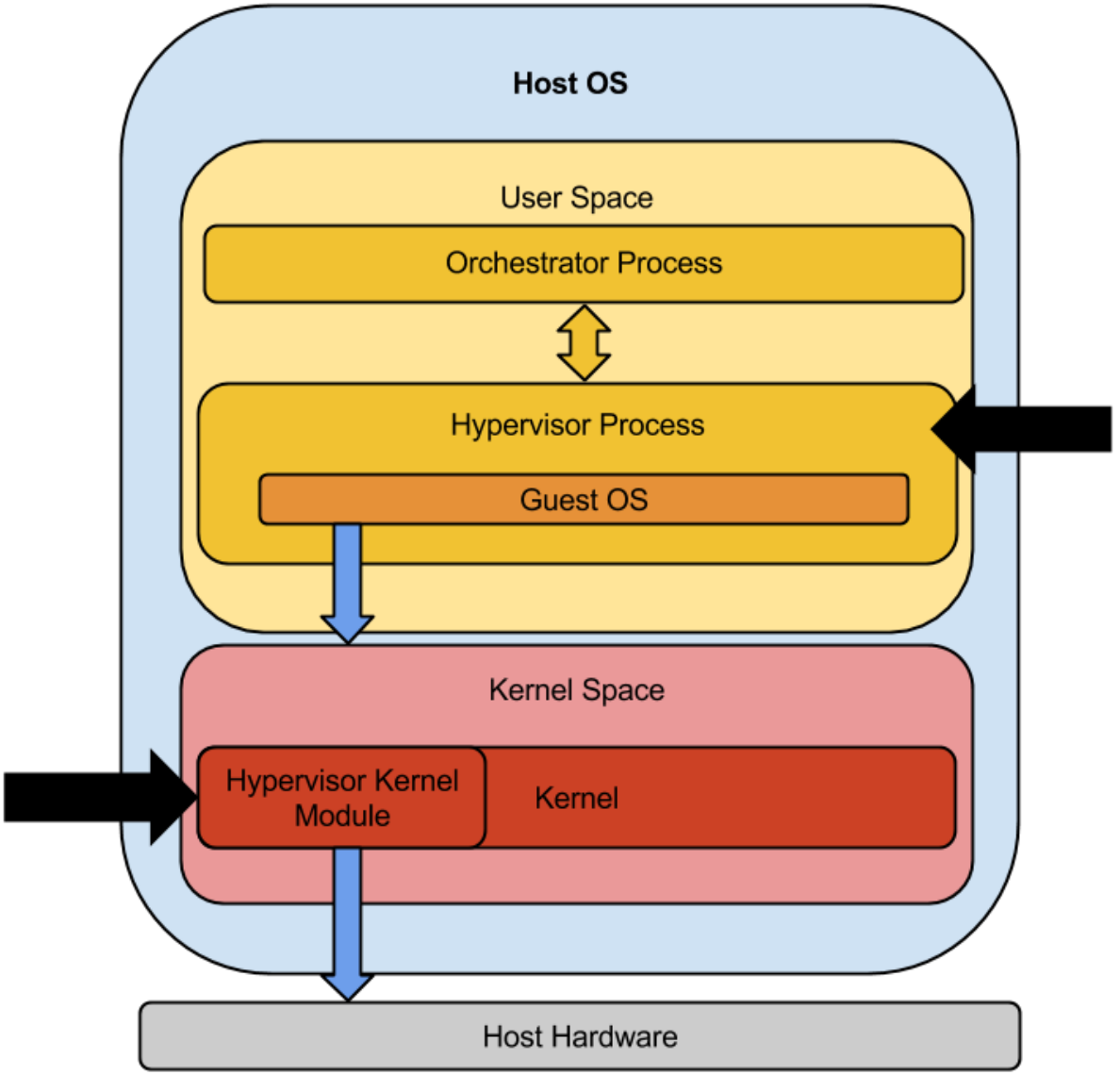
# Hypervisor

- Hypervisor emulates hardware for guest
- Hypervisor allocates some real system RAM to each VM, and shares the CPU time

# Orchestrator

- APIs for administering guest operations
  - Start / Stop
  - Creation / Destruction
  - Failover / Migration
- Examples
  - Libvirt
  - Ganeti

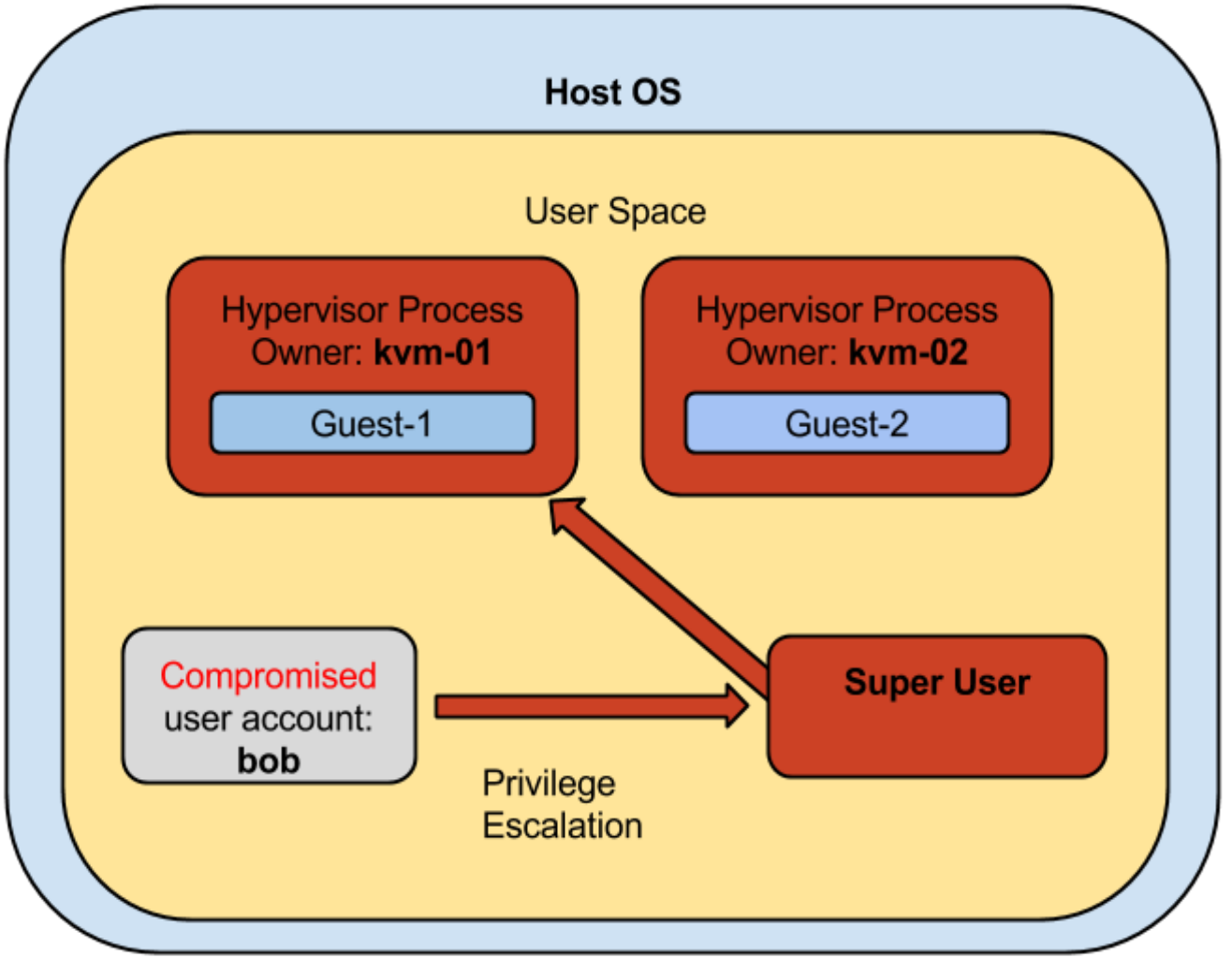
# Visualizing the Virtualization Stack



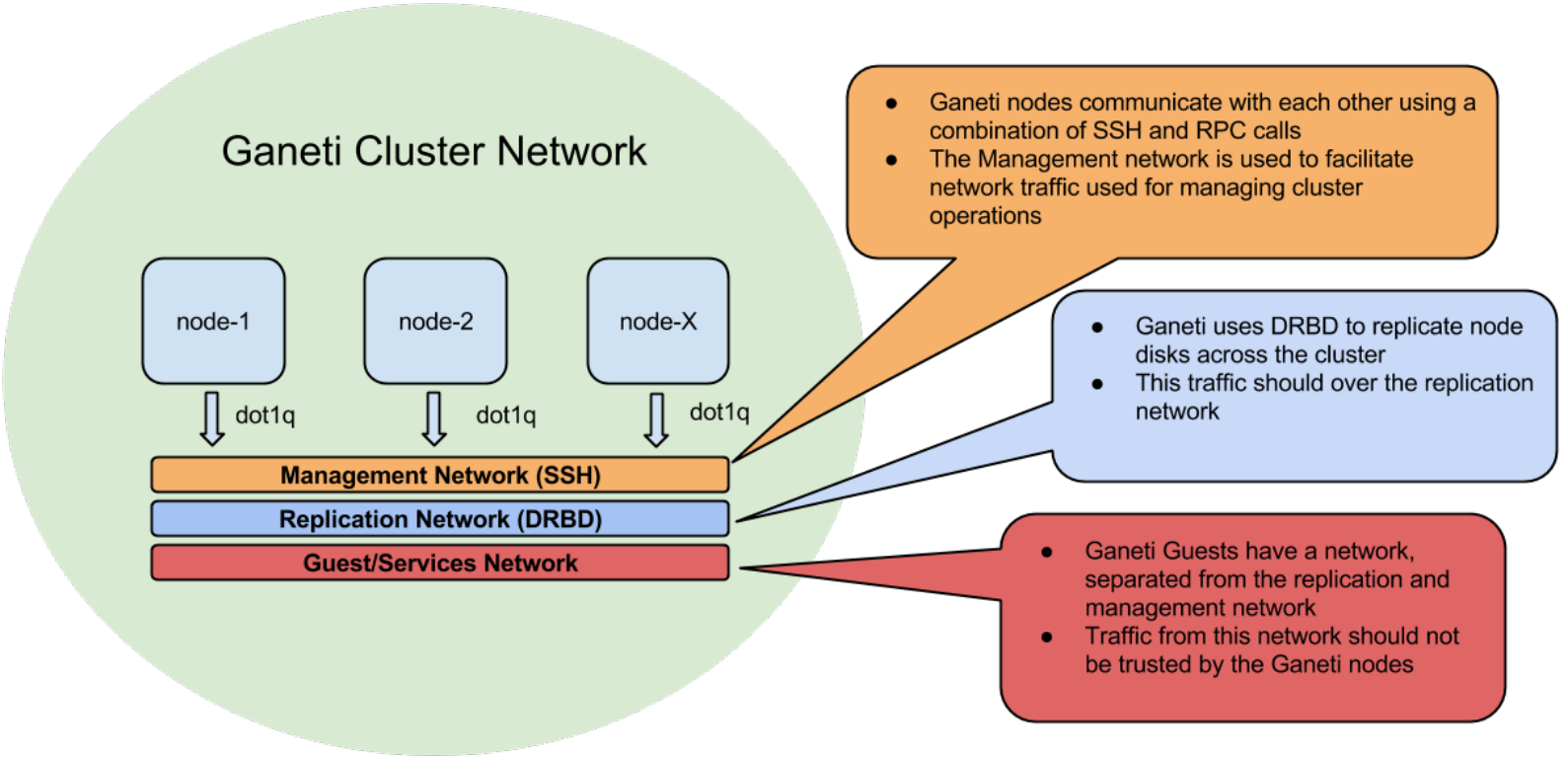
# Threat Model: What is possible?

- **Privilege Escalation**
  - Exploit that allows unprivileged subject access to guests through hypervisor, orchestrator services
- Denial of Service
  - Attacker denies other users access to shared resources

# Example:
# Escalate User Privileges, Access Guests



# Example: Guest Access Orchestrator API

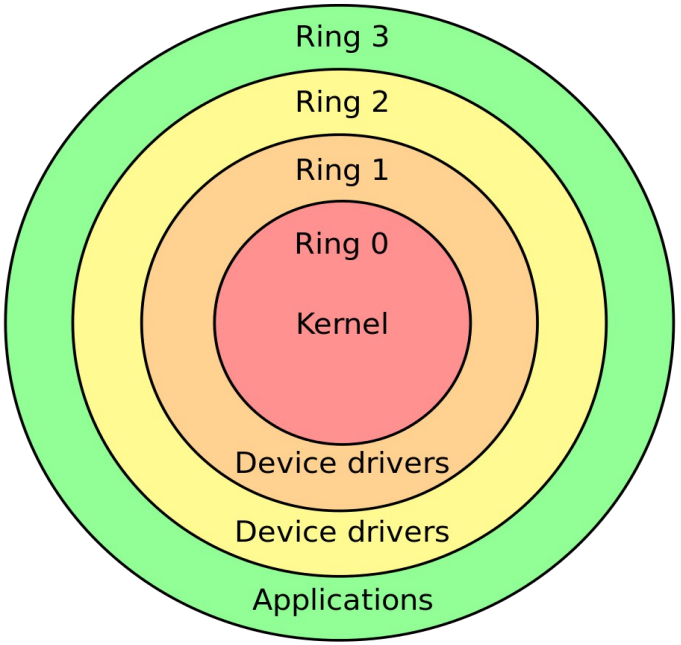


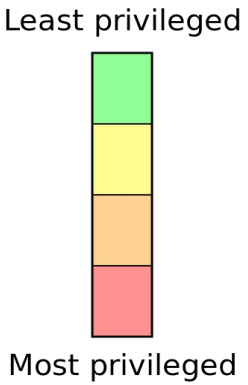
# VM Escape

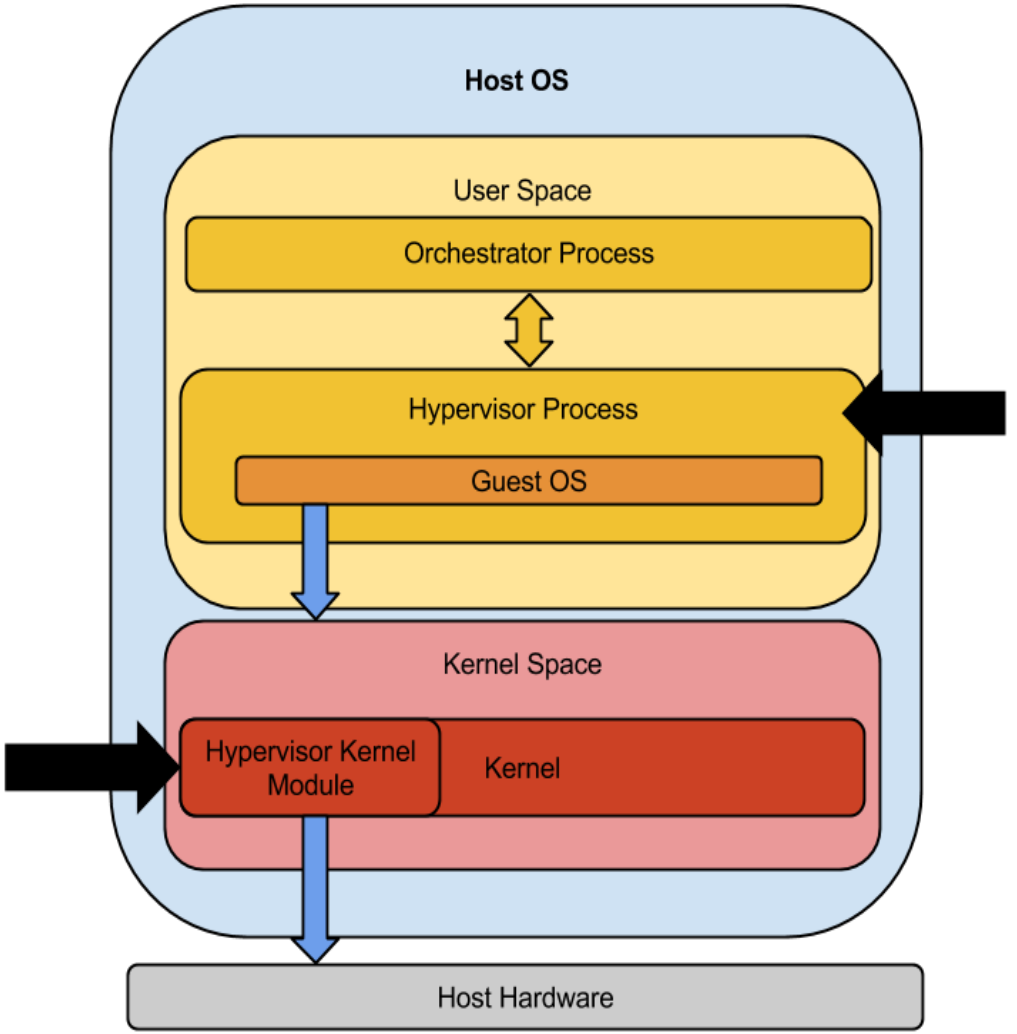
Breaking out of Guest and interacting with and/or executing code on the host.

- Spawn a shell
- Open a network backdoor
- ...

# Guests vs. Hypervisor



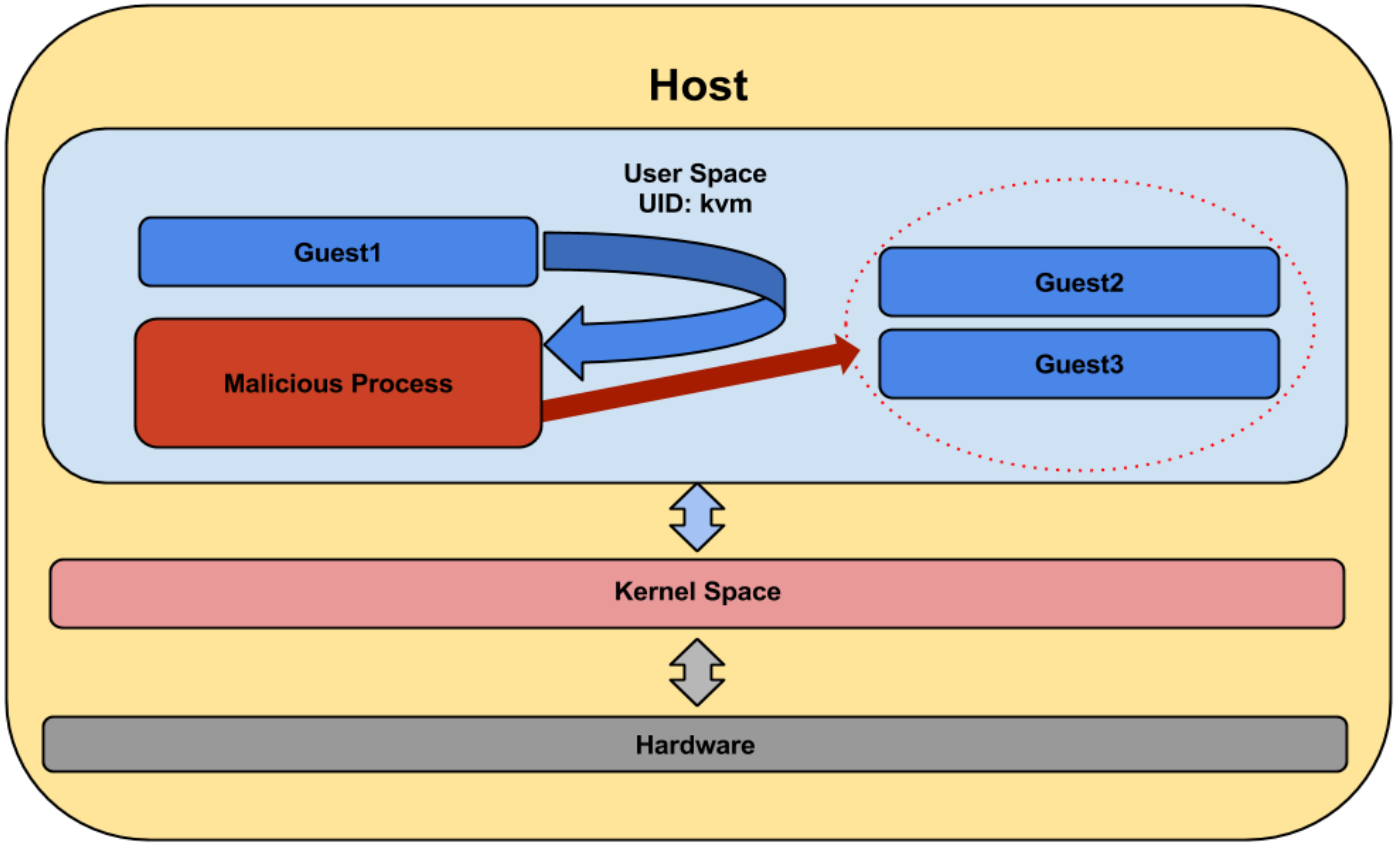



# CVE-2015-3456, “Venom”

- Flaw in emulator's implementation of Floppy controller
- Doesn't require the presence of a floppy drive on the system, just access to send I/O to controller
- Allows Guest user to execute arbitrary code in “user” space on Host

# Escape to User Space

- Attacker can execute code and access resources as the owner of the **hypervisor** process

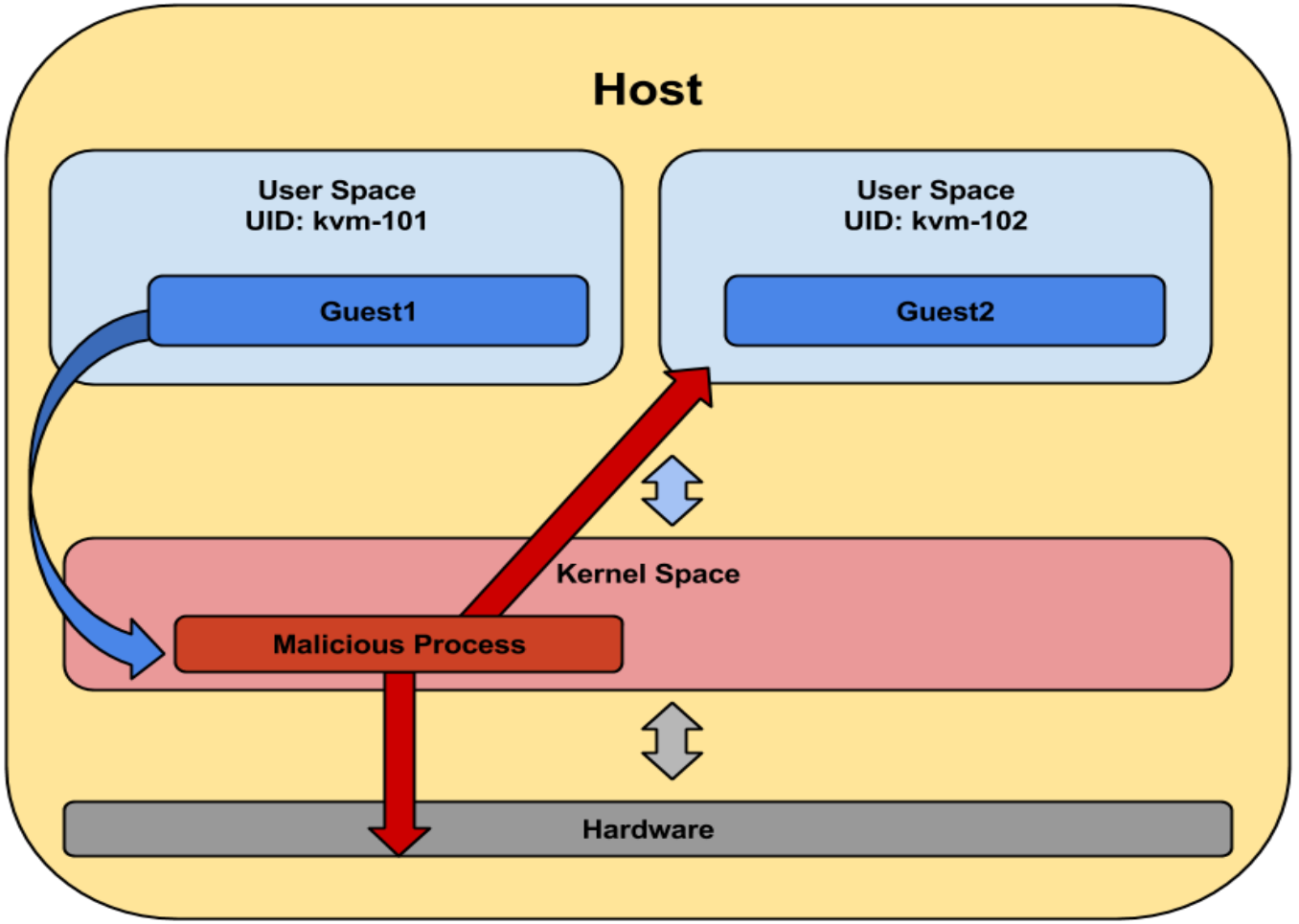


# CVE-2012-0217 kernel: x86_64

- Affects Xen Hypervisor
- When a **guest** is run paravirtualized, it runs a modified kernel that passes some instructions directly to **host** kernel
- Flaw in system call in **host** kernel that allows **guest** to execute arbitrary code in kernel space on **host**

# Escape to Kernel Space

- Attacker can execute code and access resources as the owner with Kernel privileges

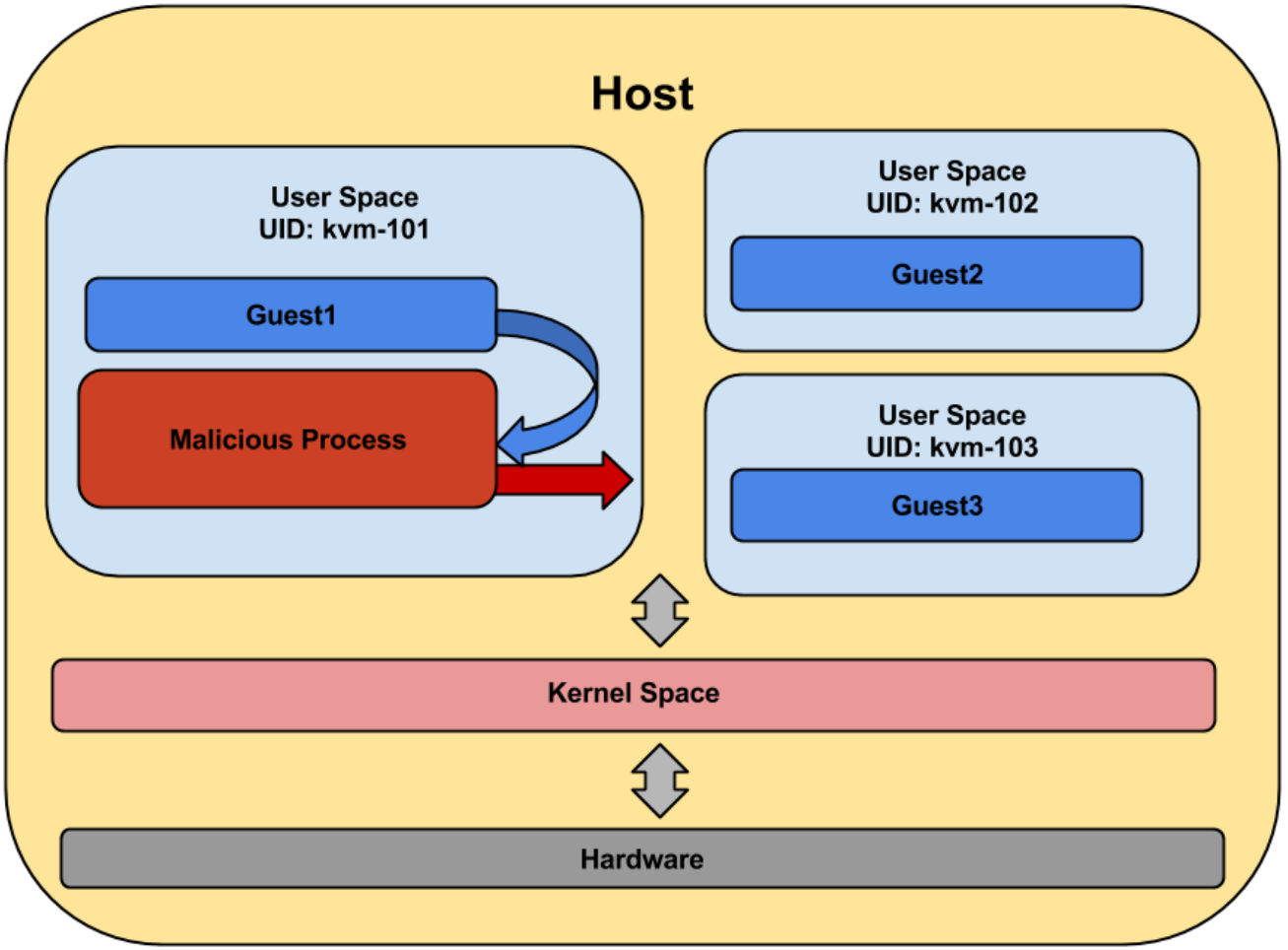


# Privilege Escalation Mitigation

# Segregate Guest Execution Space

- Execute VM's as non-privileged, service users
  - No home directories
  - No password
  - No Shell
- Allocate one user account per guest
  - In the case of VM Escape, every guest is isolated

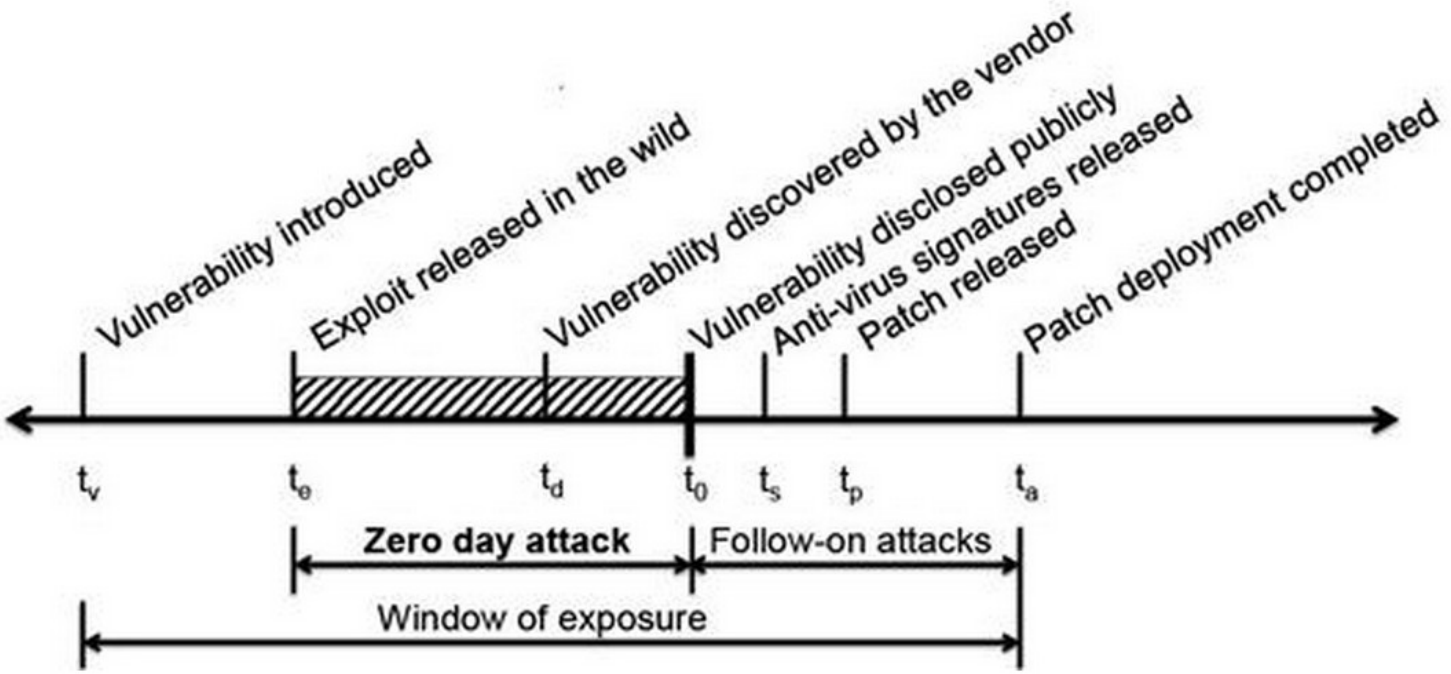
# Segregate VM Execution Space



# Patch your systems!

- Hypervisor vulnerabilities are mitigated by patches to the hypervisor software

# Mind the Vulnerability Timeline




http://blog.coresecurity.com/2013/02/27/a-world-of-vulnerabilities-guest-blog-post-from-infosec-institute/

# Audit System Logs

- Audit privilege escalation
  - Sudoers
  - Root logins
- Audit orchestrator events
  - Start / Stop / Restart Guest
  - Attach / detach storage
  - Changes to network interfaces

# Segregate Services

- Apply the principle of least privilege:
  - Which users need access to the host? Guests?
  - What network communication is strictly necessary?
  - What communication channels could jeopardize hypervisor?
  - What communication channels could jeopardize data?

# Harden Network Services

- Enable authentication and encryption for remote access protocols
  - VNC
  - Orchestrator APIs
- Isolate Guest network from Host network
- Scope the listening interfaces for network services where possible

# Summary

- Virtualization has many benefits but it can be major privilege escalation vector if managed improperly
- Patching accompanied by strong access control around the hypervisor and orchestrator can limit the damage caused by privilege escalation
- Auditing and monitoring orchestrator and OS logs will help you know when and if you are being attacked and perhaps even if the attack was successful