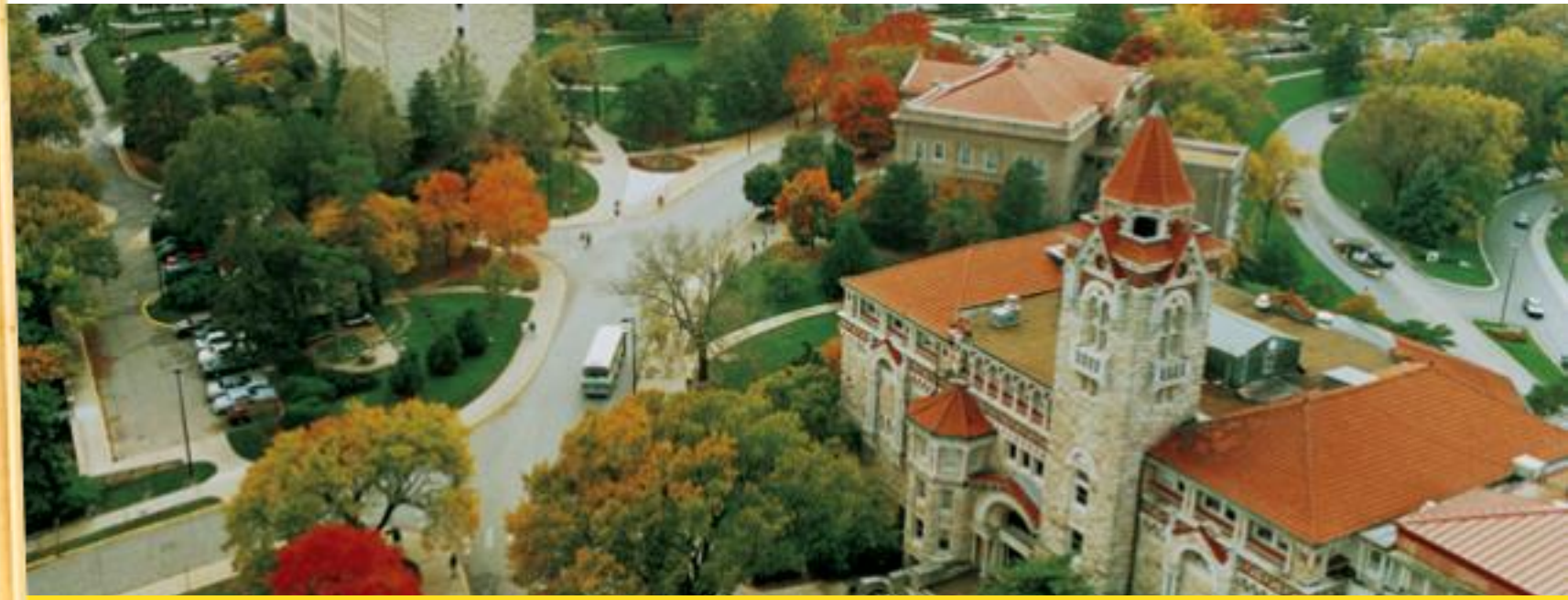
Cloud Computing Security

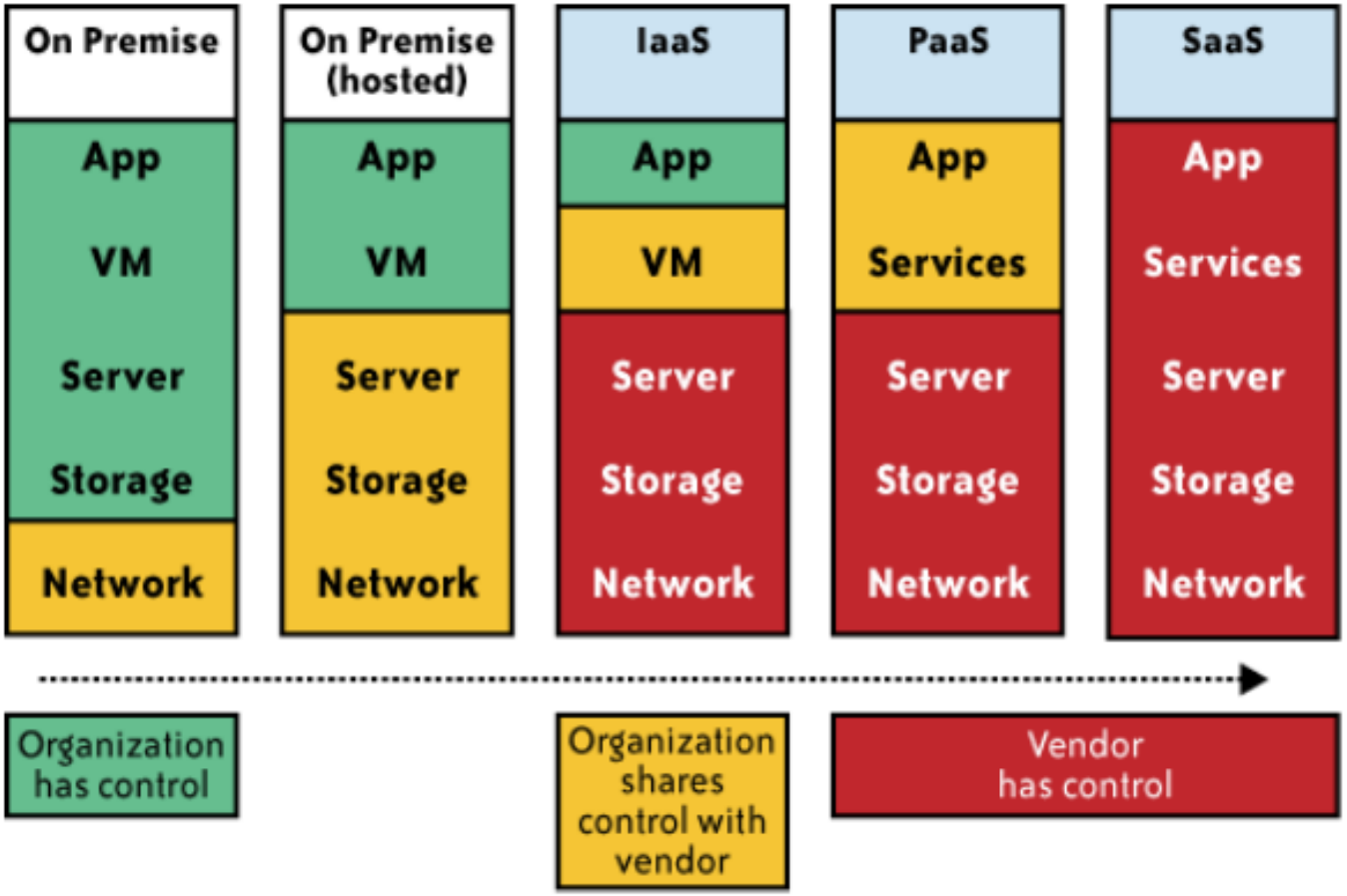


Cloud Models

- Delivery Models
  - SaaS: Software as a service
  - PaaS: Platform as a service
  - IaaS: Infrastructure as a service
- Deployment Models
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud
- Management Models (trust and tenancy issues)
  - Self-managed
  - 3rd party managed (e.g. public clouds and VPC)

From [1] NIST

Cloud Models



From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Quote of the day

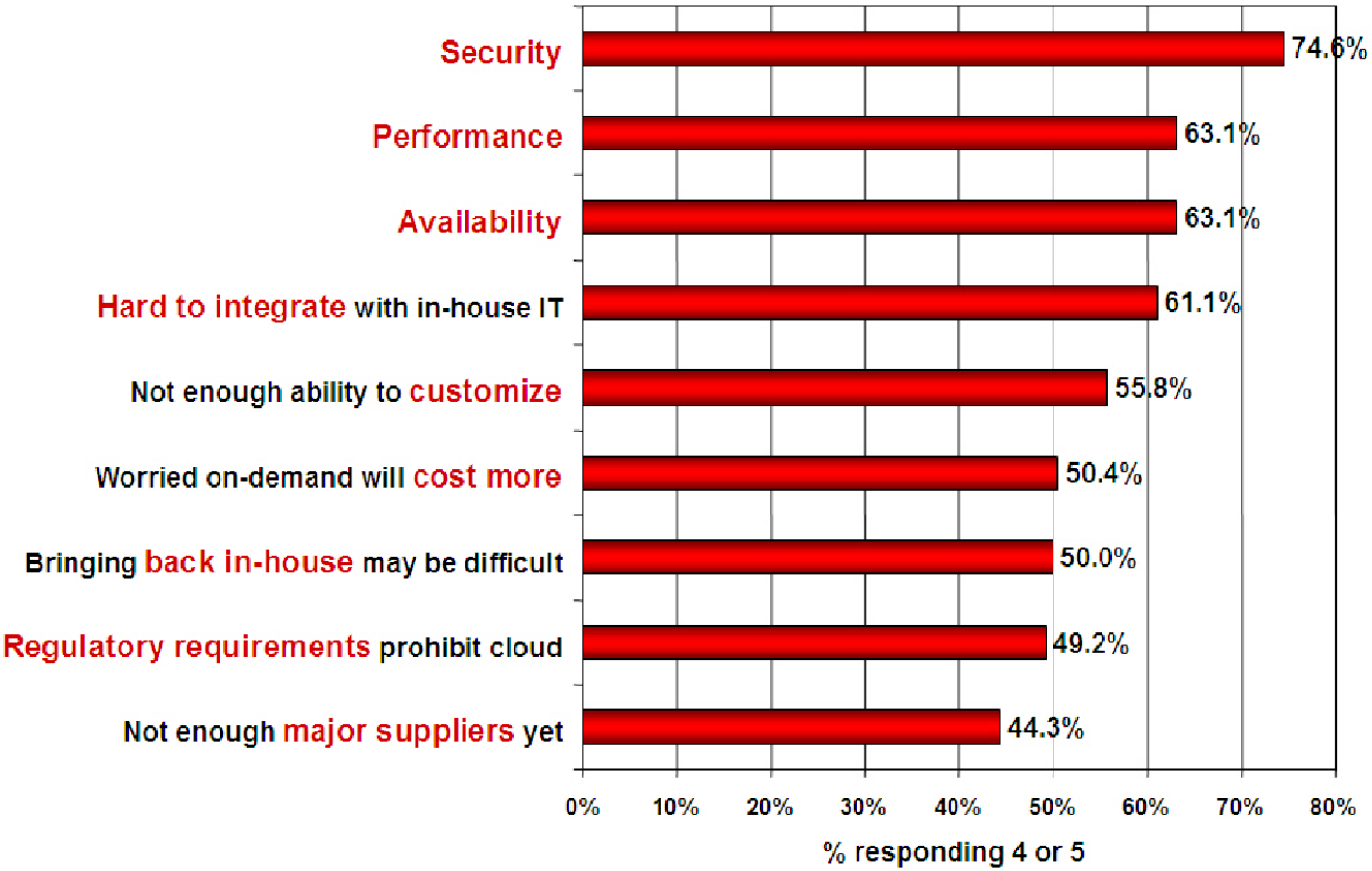
[Cloud Computing] is a **security nightmare** and it can't be handled in traditional ways.

John Chambers
CISCO CEO

Companies are afraid to use clouds

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

Security problems in cloud computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
- Self-managed clouds still have security issues, but not related to above

Anatomy of fear …

- Confidentiality
  - Will the sensitive data stored on a cloud remain confidential? Will cloud compromises leak confidential client data (i.e., fear of loss of control over data)
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?
- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?

Anatomy of fear …

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

Anatomy of fear …

- Auditability and forensics
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations (e.g., SOX, HIPAA, GLBA)?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

Why Cloud Computing brings new threats?

- Clouds allow co-tenancy
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

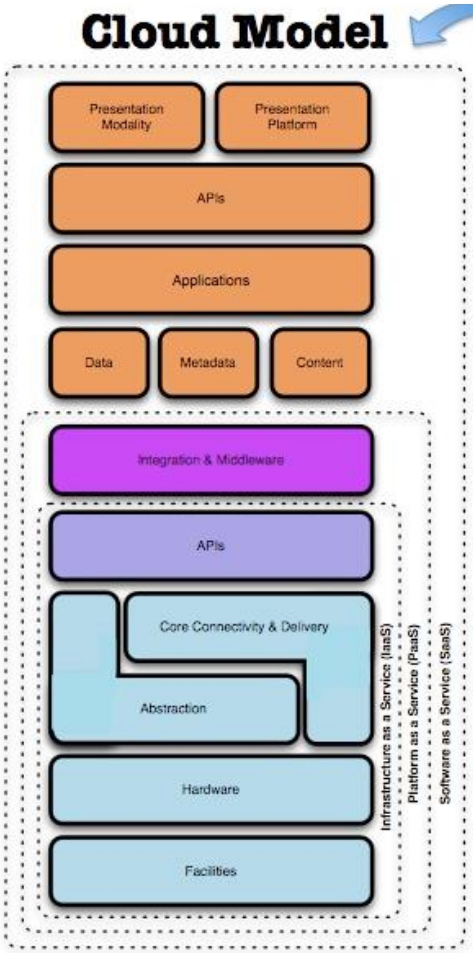
Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

Case study: Amazon's EC2 infrastructure

- “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds”
  - Multiple VMs of different organizations with virtual boundaries separating each VM can run within one physical server
  - "virtual machines" still have internet protocol, or IP, addresses, visible to anyone within the cloud.
  - VMs located on the same physical server tend to have IP addresses that are close to each other and are assigned at the same time
  - An attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target
  - Once the malicious virtual machine is placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim

Security Interaction Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- Firewalls
- Code Review
- WAF
- Encryption
- Unique User IDs
- Anti-Virus
- Monitoring/IDS/IPS
- Patch/Vulnerability Management
- Physical Access Control
- Two-Factor Authentication...

HIPAA

GLBA

SOX

Top Security Threats

- Abuse and nefarious use of cloud computing
- Insecure interfaces & API's
- Unknown risk profile
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking

Threat Mitigation

Abuse and nefarious use of cloud computing	▪ Stricter initial registration and validation processes. ▪ Enhanced credit card fraud monitoring and coordination. ▪ Comprehensive introspection of customer network traffic. ▪ Monitoring public blacklists for one's own network blocks.
Insecure interfaces & API's	▪ Analyze the security model of cloud provider interfaces. ▪ Ensure strong authentication and access controls are implemented in concert with encrypted transmission. ▪ Understand the dependency chain associated with the API.
Unknown risk profile	▪ Disclosure of applicable logs and data. Partial/full disclosure of infrastructure details ▪ Monitoring and alerting on necessary information.

Threat Mitigation

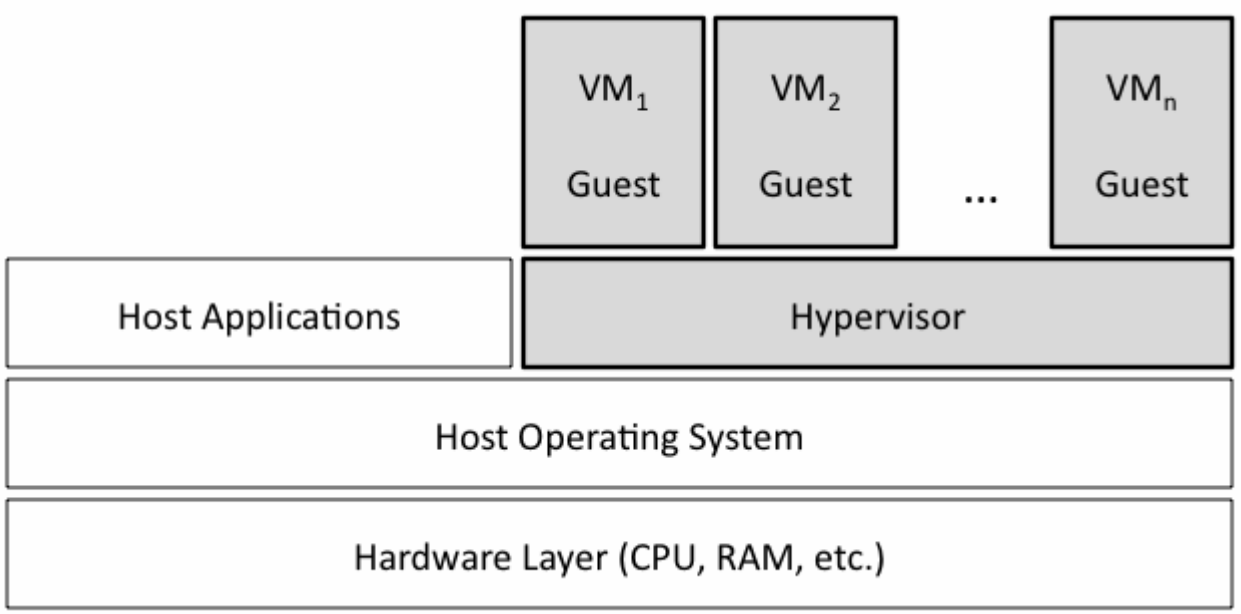
Malicious insiders	▪ Enforce strict supply chain management and conduct a comprehensive supplier assessment. ▪ Specify human resource requirements as part of legal contracts. ▪ Require transparency into overall information security and management practices, as well as compliance reporting. ▪ Determine security breach notification processes.
Shared technology issues	▪ Implement security best practices for installation and configuration. ▪ Monitor environment for unauthorized changes/activity. ▪ Promote strong authentication and access control for administrative access and operations. ▪ Enforce service level agreements for patching and vulnerability remediation. ▪ Conduct vulnerability scanning and configuration audits.

Threat Mitigation

Data loss or leakage	▪ Implement strong API access control. ▪ Encrypt and protect integrity of data in transit. ▪ Analyze data protection at both design and run time. ▪ Implement strong key generation, storage and management, and destruction practices. ▪ Contractually demand providers wipe persistent media before it is released into the pool. ▪ Contractually specify provider backup and retention strategies.
Account or service hijacking	▪ Prohibit the sharing of account credentials between users and services. ▪ Leverage strong two-factor authentication techniques where possible. ▪ Employ proactive monitoring to detect unauthorized activity. ▪ Understand cloud provider security policies and SLAs.

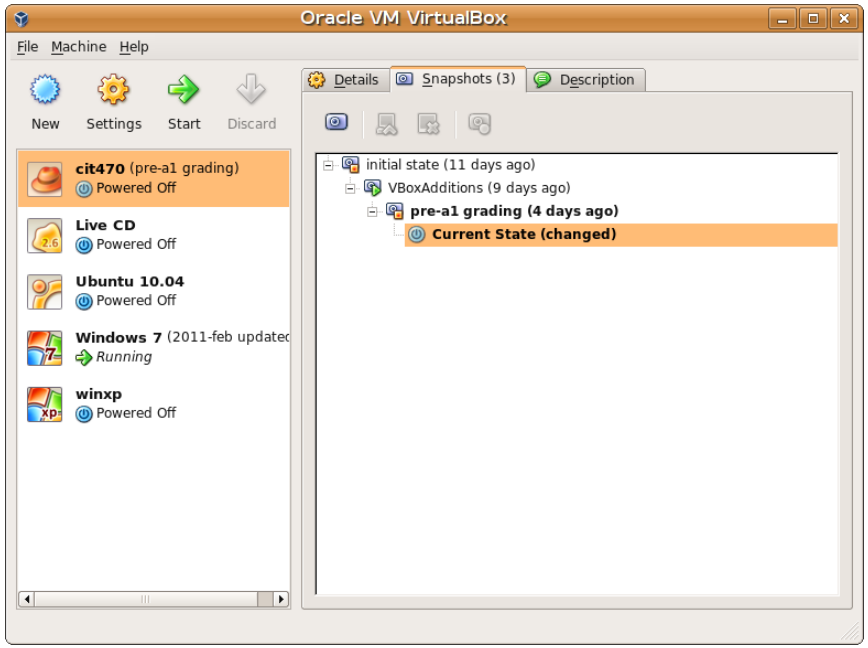
Virtualization Security Features: Isolation

- Using a VM for each application provides isolation
  - More than running 2 apps on same server.
  - Less than running on 2 physical servers



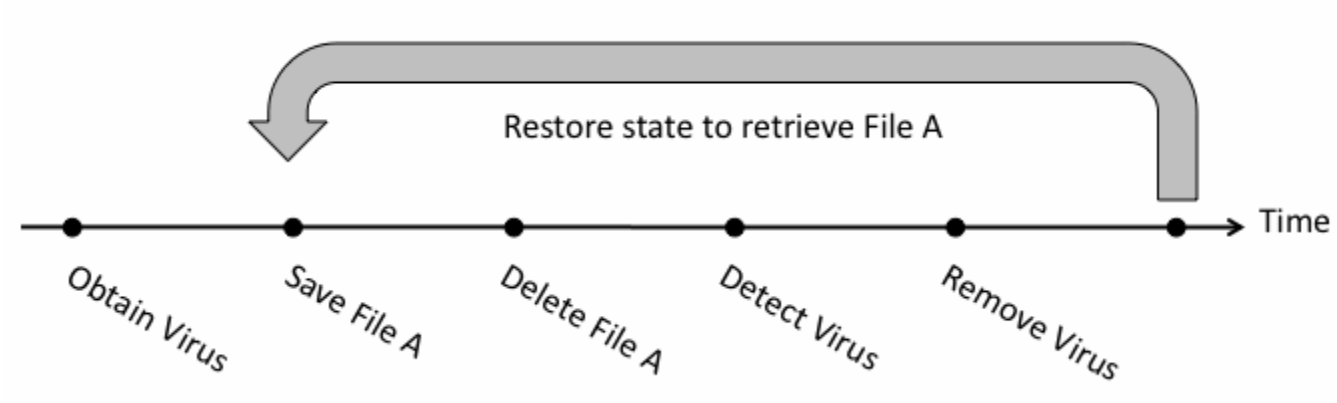
Virtualization Security Features: Snapshot

- VMs can record state.
- In event of security incident, revert VM back to an uncompromised state.
- Must be sure to patch VM to avoid recurrence of compromise.



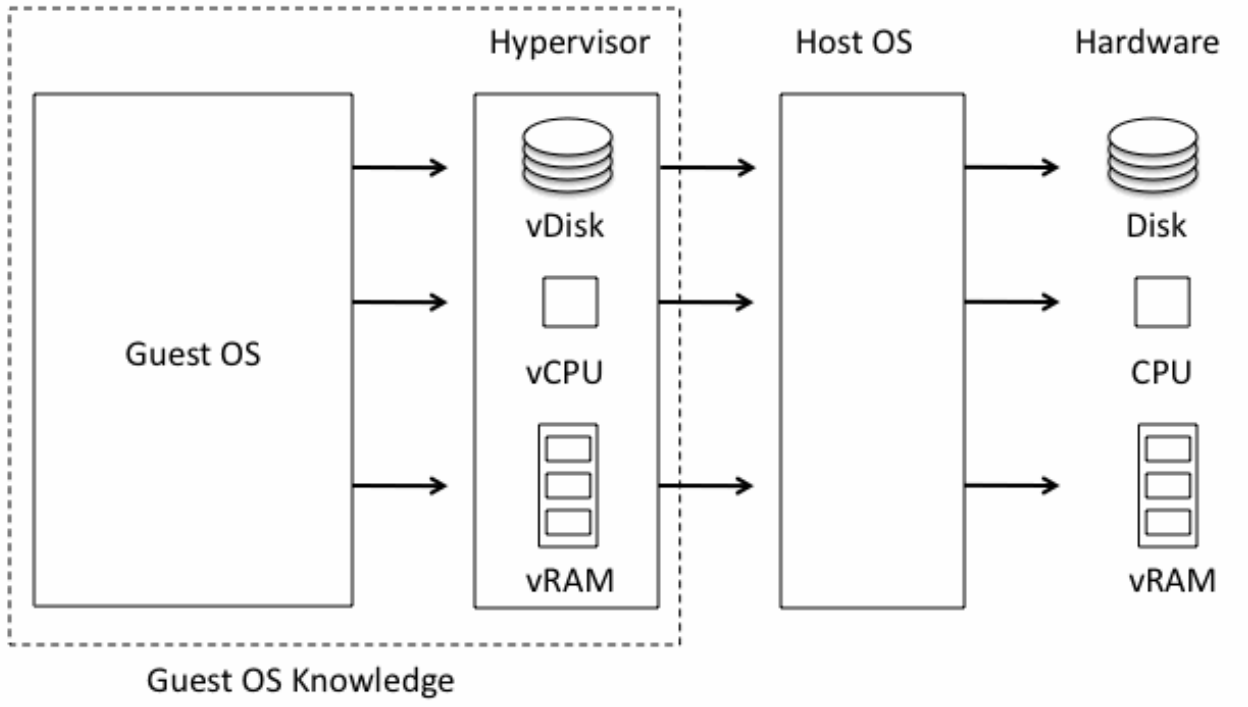
State Restore

- VMs can be restored to an infected or vulnerable state using snapshots.
- Patching becomes undone.
- Worms persist at low level forever due to reappearance of infected and vulnerable VMs.



Complexity

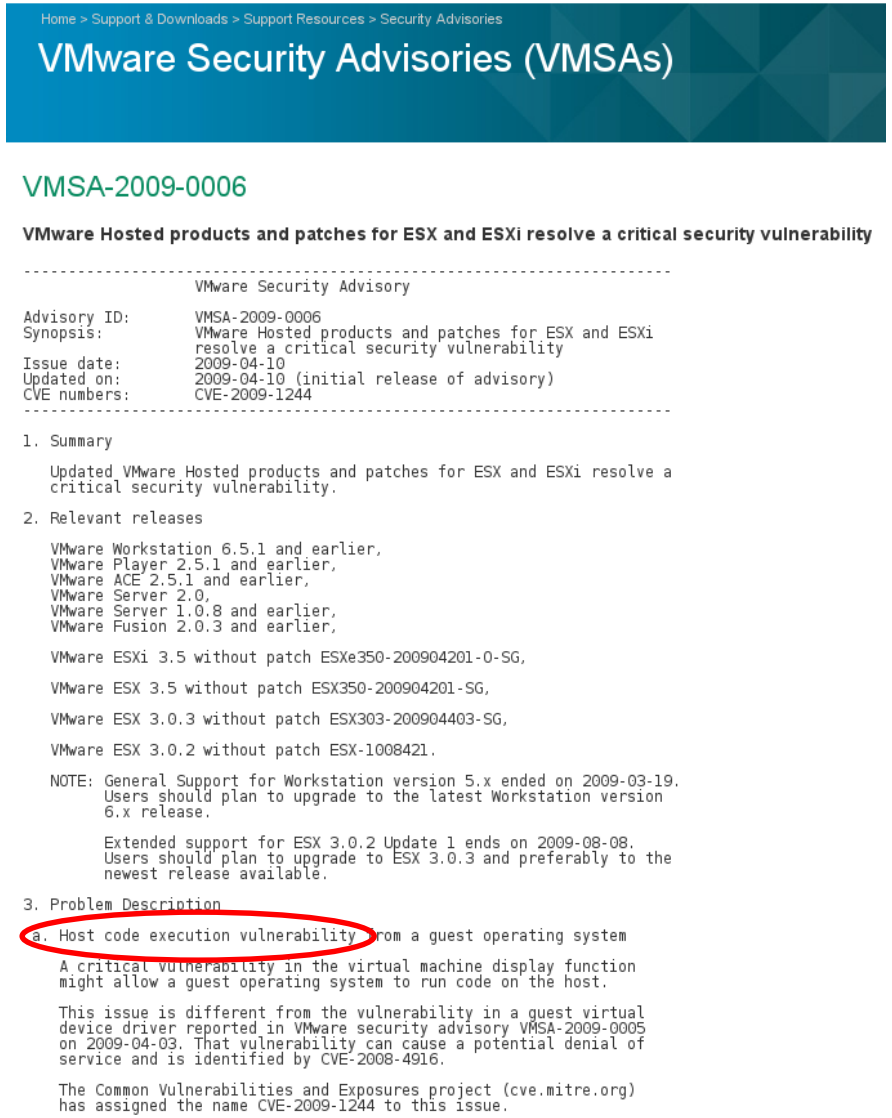
- Hypervisor may be simple or not, but
- It is often another layer on top of host OS, adding complexity and vulnerabilities.



Hypervisor Security

- Vulnerability consequences
  - Guest code execution with privilege
  - VM Escape (Host code execution)

Vendor	CVEs
KVM	32
QEMU	23
VirtualBox	9
VMware	126
Xen	86



Home > Support & Downloads > Support Resources > Security Advisories

VMware Security Advisories (VMSAs)

VMSA-2009-0006

VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability

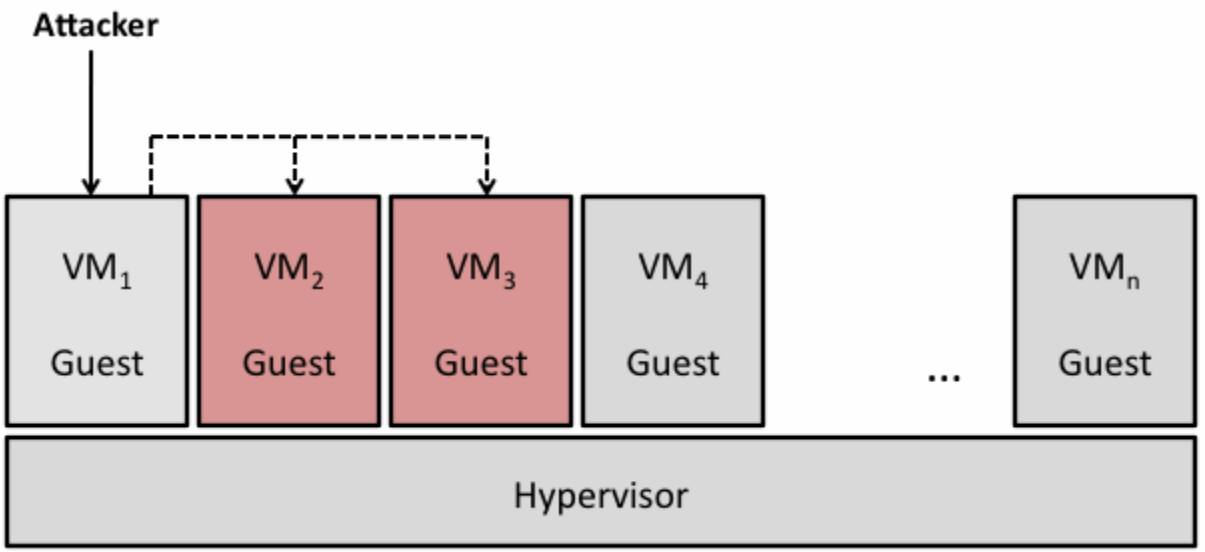
```
-------------------------------------------------------------------------
                   VMware Security Advisory

Advisory ID:       VMSA-2009-0006
Synopsis:          VMware Hosted products and patches for ESX and ESXi
                   resolve a critical security vulnerability
Issue date:        2009-04-10
Updated on:        2009-04-10 (initial release of advisory)
CVE numbers:       CVE-2009-1244
-------------------------------------------------------------------------

1. Summary

   Updated VMware Hosted products and patches for ESX and ESXi resolve a
   critical security vulnerability.

2. Relevant releases

   VMware Workstation 6.5.1 and earlier,
   VMware Player 2.5.1 and earlier,
   VMware ACE 2.5.1 and earlier,
   VMware Server 2.0,
   VMware Server 1.0.8 and earlier,
   VMware Fusion 2.0.3 and earlier,

   VMware ESXi 3.5 without patch ESXe350-200904201-O-SG,

   VMware ESX 3.5 without patch ESX350-200904201-SG,

   VMware ESX 3.0.3 without patch ESX303-200904403-SG,

   VMware ESX 3.0.2 without patch ESX-1008421.

   NOTE: General Support for Workstation version 5.x ended on 2009-03-19.
         Users should plan to upgrade to the latest Workstation version
         6.x release.

         Extended support for ESX 3.0.2 Update 1 ends on 2009-08-08.
         Users should plan to upgrade to ESX 3.0.3 and preferably to the
         newest release available.

3. Problem Description

a. Host code execution vulnerability from a guest operating system

   A critical vulnerability in the virtual machine display function
   might allow a guest operating system to run code on the host.

   This issue is different from the vulnerability in a guest virtual
   device driver reported in VMware security advisory VMSA-2009-0005
   on 2009-04-03. That vulnerability can cause a potential denial of
   service and is identified by CVE-2008-4916.

   The Common Vulnerabilities and Exposures project (cve.mitre.org)
   has assigned the name CVE-2009-1244 to this issue.
```

Xen CVE-2008-1943
VBox CVE-2010-3583

THE UNIVERSITY OF KANSAS

Inter-VM Attacks

- Attack via shared clipboard
  - http://www.securiteam.com/securitynews/5GP021FKKO.html
- Use shared folder to alter other VM's disk image
  - CVE-2007-1744



Scaling

- Growth in physical machines limited by budget and setup time.
- Adding a VM is easy as copying a file, leading to explosive growth in VMs.
- Rapid scaling can exceed capacity of organization's security systems.

Transience

- Users often have specialized VMs.
  - Testing
  - Different app versions
  - Demos
  - Sandbox
- that are not always up, preventing network from converging to a known state.
  - Infected machines appear, attack, then disappear from the network before can be detected.
  - Vulnerable systems likewise appear too briefly to be detected and patched.

Data Lifetime

- Although data was correctly sanitized from VM disk and/or memory, snapshots can retain multiple copies of both VM memory and disk data.