Playing by Virtual Security Rules: How Virtualization Changes Everything and What to Do about It

Steve Pate

CTO

Vormetric

Agenda

- Virtualization state of play
- Do old security rules still apply?
- Vulnerabilities with OS virtualization
- How can I protect my virtualization environment today?
- What's the virtualization security roadmap?

Where are we today?

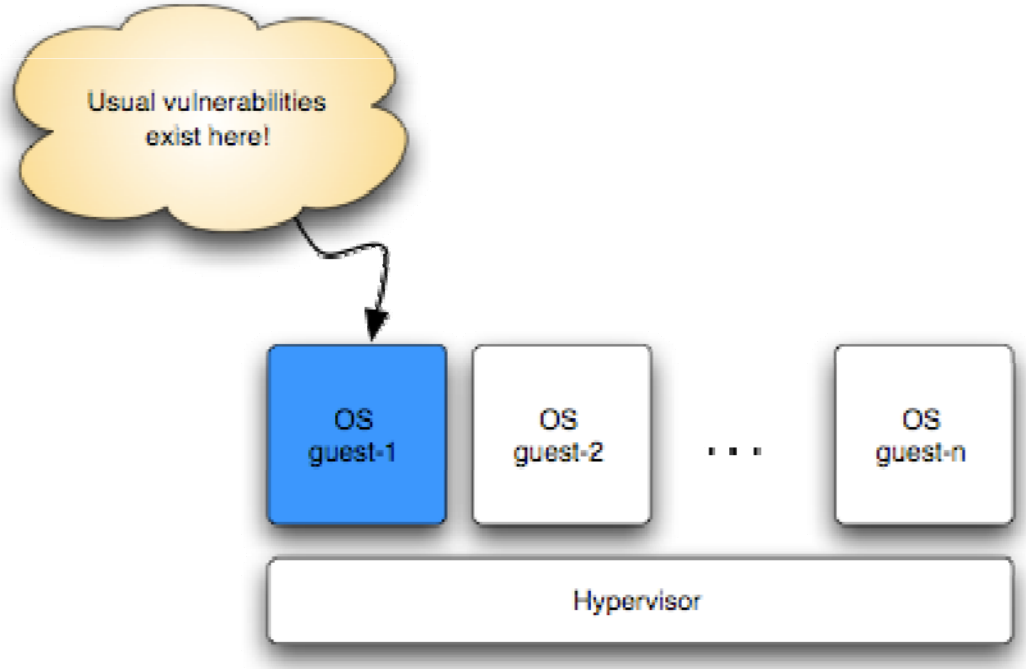
- OS virtualization moving rapidly into production environments
- Companies concerned about security issues and lack of security products
- VMware will dominate for the next few years
  - therefore the main focus of attack!
  - more security violations in Nov 07 than whole of company's history
- Hyper-V will make headway but slowly ...
- Xen will stay a distant 3rd

Changing the Security Landscape

- Defense in depth model has inherently changed
  - Physical security
  - Disk encryption
  - Vulnerability management
- Standards and best practices don't address virtualization security issues!
  - NIST
  - ISO-17799/27001
  - Regulations – PCI DSS, HIPAA

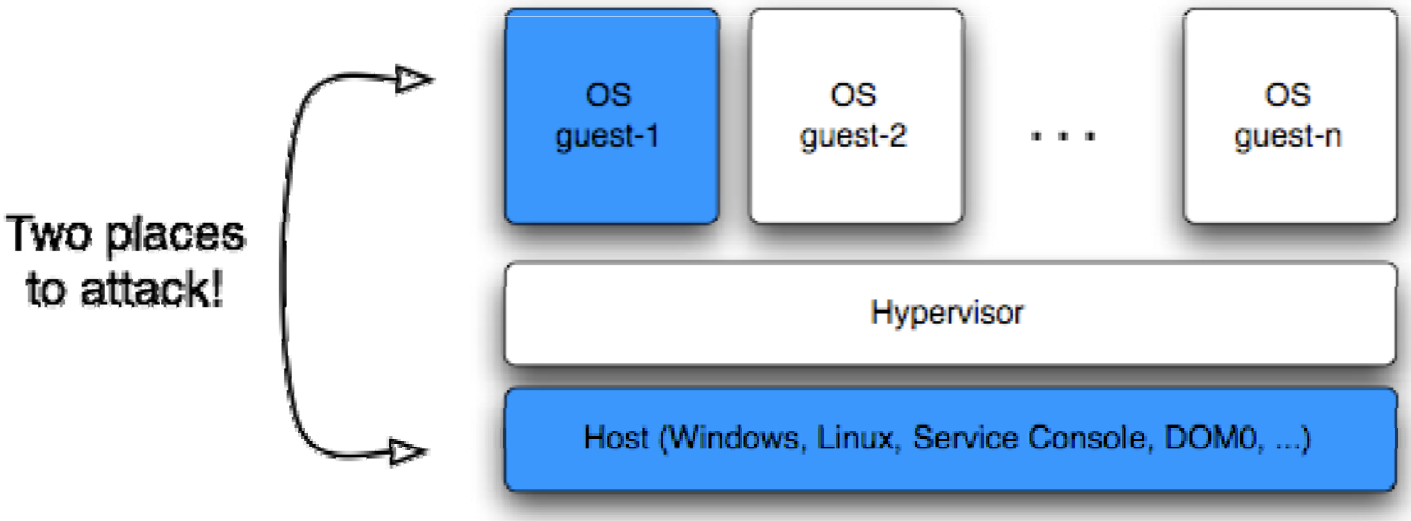
Virtualization vulnerabilities

- We must not ignore protection in the guest!
  - Traditional security problems are unchanged



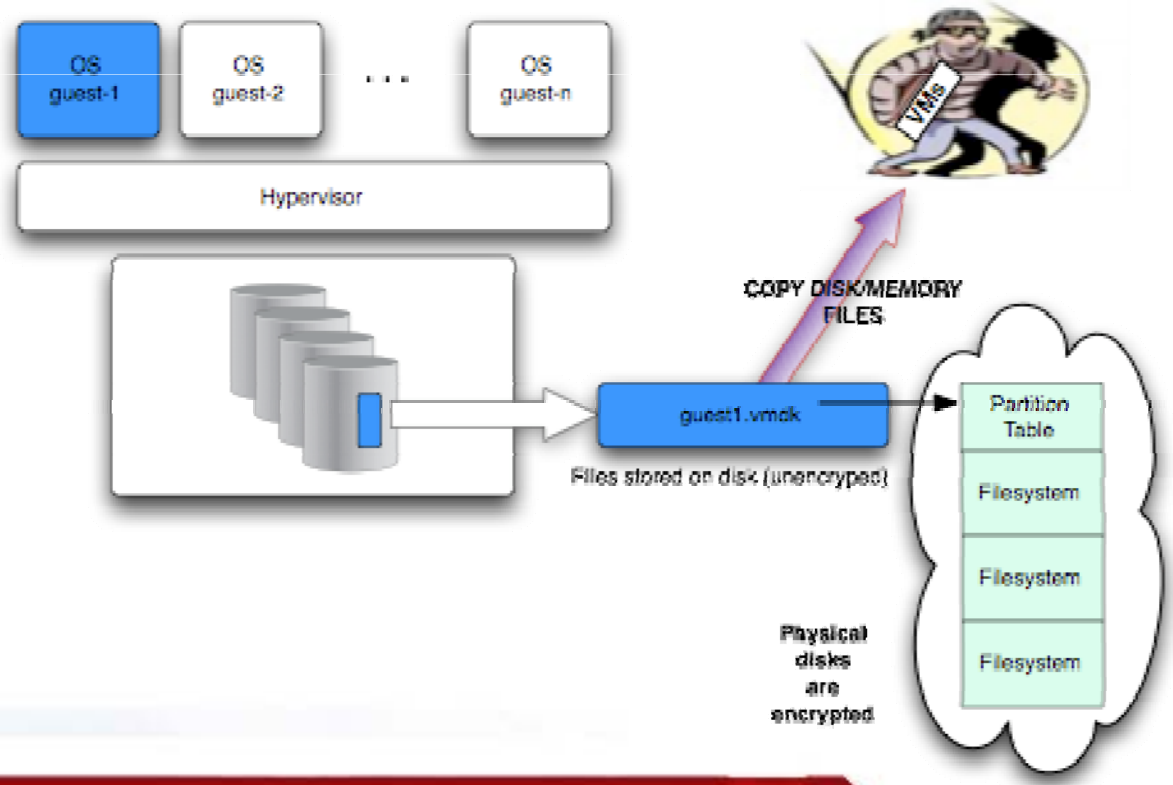
Guest and Host are vulnerable!

- Two operating systems now need protecting!



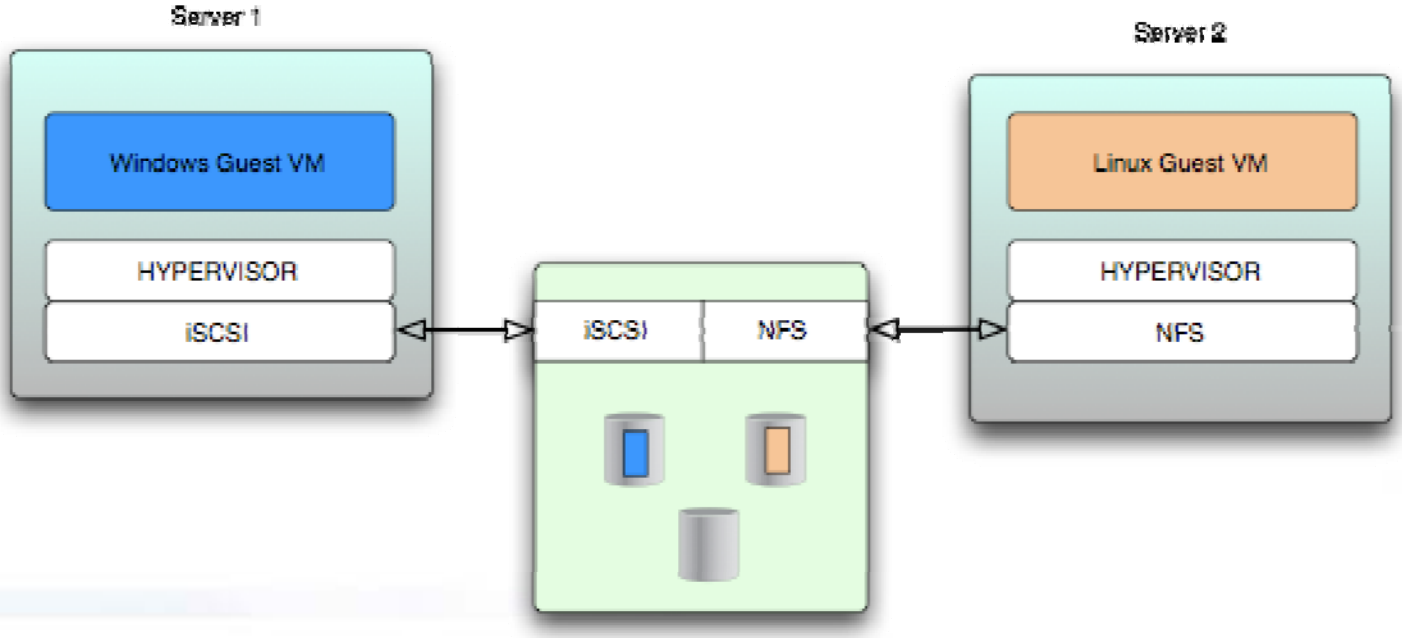
Full disk encryption?

- How useful is this?
  - Physical disk theft now means something different!



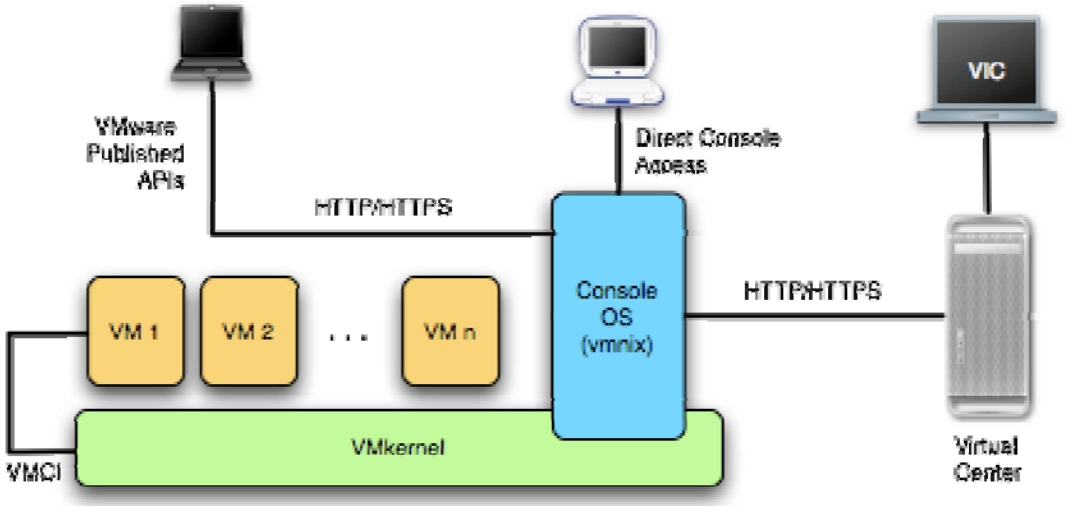
VM archives present new challenges

- How can we provide separation of duties here?
- How do I know where my VMs are located?
- How can I manage old VM images?
- How can I retire Virtual Machines?



The list of issues continues ...

- Hypervisor vulnerabilities
- VI infrastructure
  - Roles within virtual center
  - API set usable from any client
  - Lots of ESX Server Service Console issues



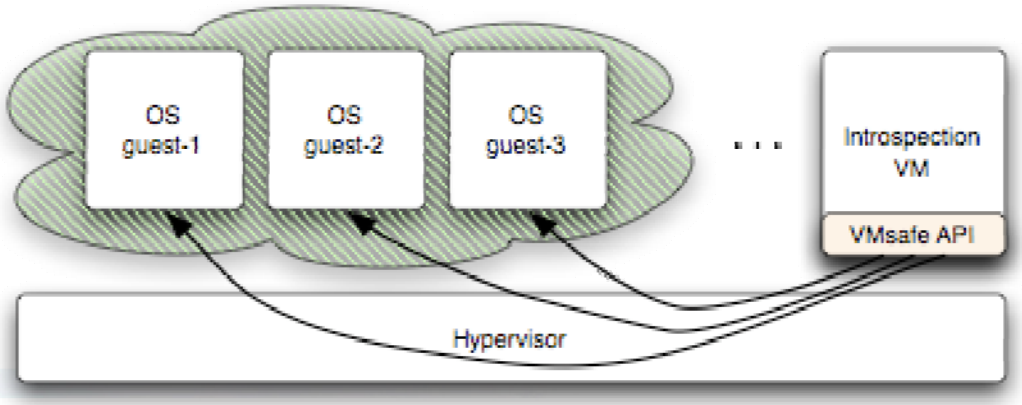
- Same issues exist with Dom0 on Xen
- Lack of solid auditing capabilities

Solutions available today?

- Traditional guest level protection!
- VMware
  - ESXi (Embedded hypervisor)
  - Determina
  - Tripwire ConfigCheck
  - Appliance Marketplace
- Xen
  - sHype (MAC capabilities)
  - XSM (LSM derivative)
- VM image encryption
- Best practices guides
  - CIS 75+ page guide for securing ESX server
  - Extensive best practices doc from VMware / Xen

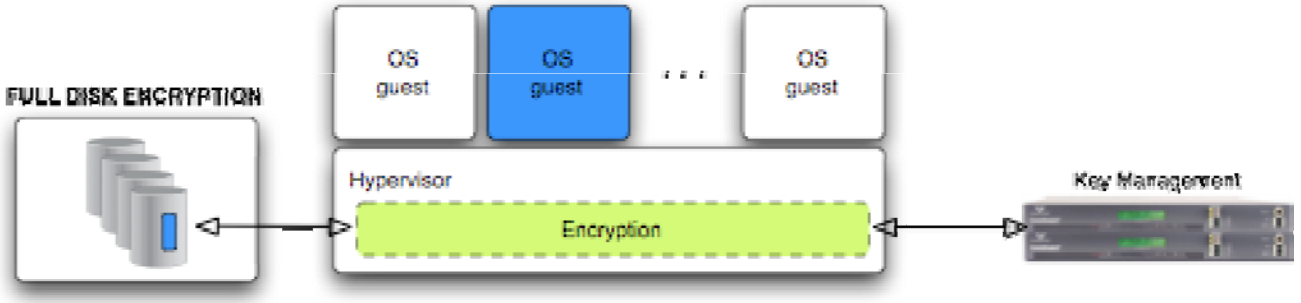
Solutions of tomorrow?

- VMsafe
  - APIs at hypervisor layer - “provides the transparency to prevent threats and attacks such as viruses, trojans and keyloggers from ever reaching a virtual machine”
  - Allows for introspection
  - 20+ vendors signed up for program
  - Products expected within the next year



Solutions of tomorrow ...

- VMware Pluggable Core Storage Architecture
  - Embedded hypervisor encryption



- Protecting the whole virtual infrastructure
  - VMware VI through Virtual Center to the ESX servers
  - Consistent access control across the whole environment
  - Full auditing

Solutions of tomorrow ...

- Security info embedded in OVF
  - OVF wraps VM images
    - Describes resources needed by VM
  - Embed key and policy information
    - Defines security requirements for VM
    - Allows VMs to expire
  - Tamper free stamp

Summary

- Protect the guest!
  - While running and at rest!
- Follow best practices
- Put strict policies in place - enforce them!
- Stay educated - this space is moving fast!

Questions?

spate@vormetric.com

www.vormetric.com