Virtual Reality: How Secure Is Your Virtualised Network

Gunter Ollmann
Chief Security Strategist

a Corman
ncipal Security Strategist

IBM Internet Security Systems®
Ahead of the threat.™

vb 2008 OTTAWA

10/2/2008

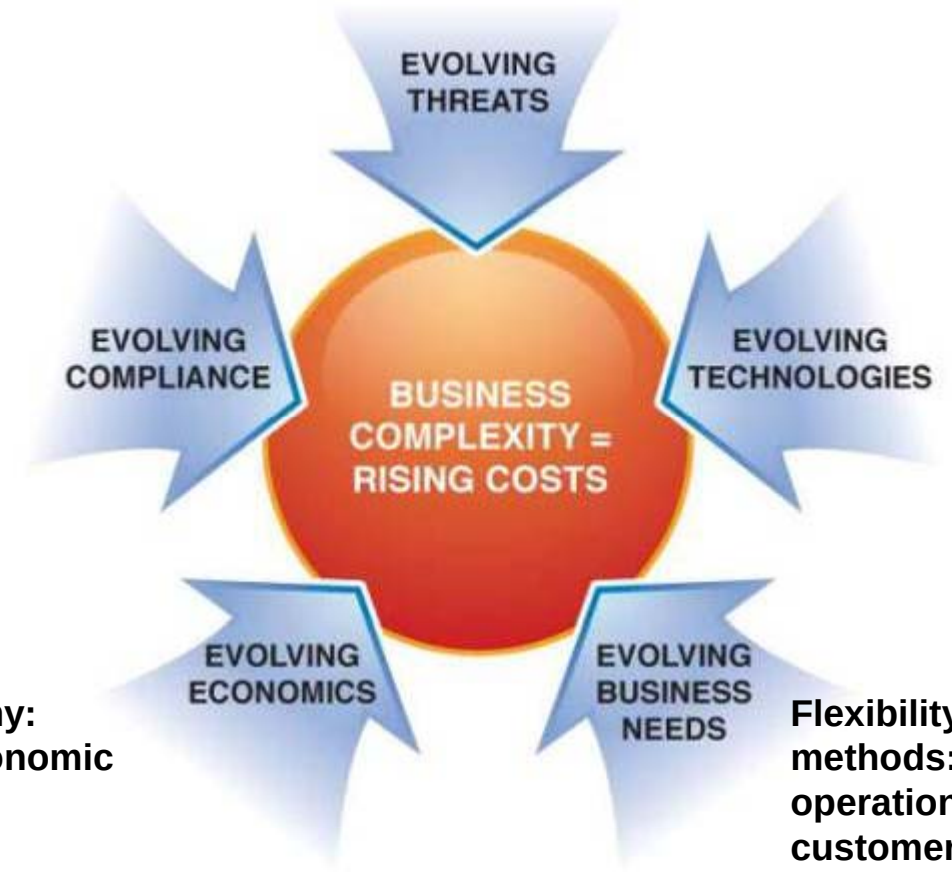
Agenda

- **Introduction to Virtualization**
- **Security and Risk Implications**
- **Operational and Organizational Implications**
- **Common Mistakes**
- **What Can I Do?**
  - Current technologies and solutions
  - The future of virtualization and enterprise security

Foreword: Unprecedented Cost and Complexity

New methods and motives: adding to the complexity and sheer number of risks

Compliance spending: investing in more point products to solve more point problems



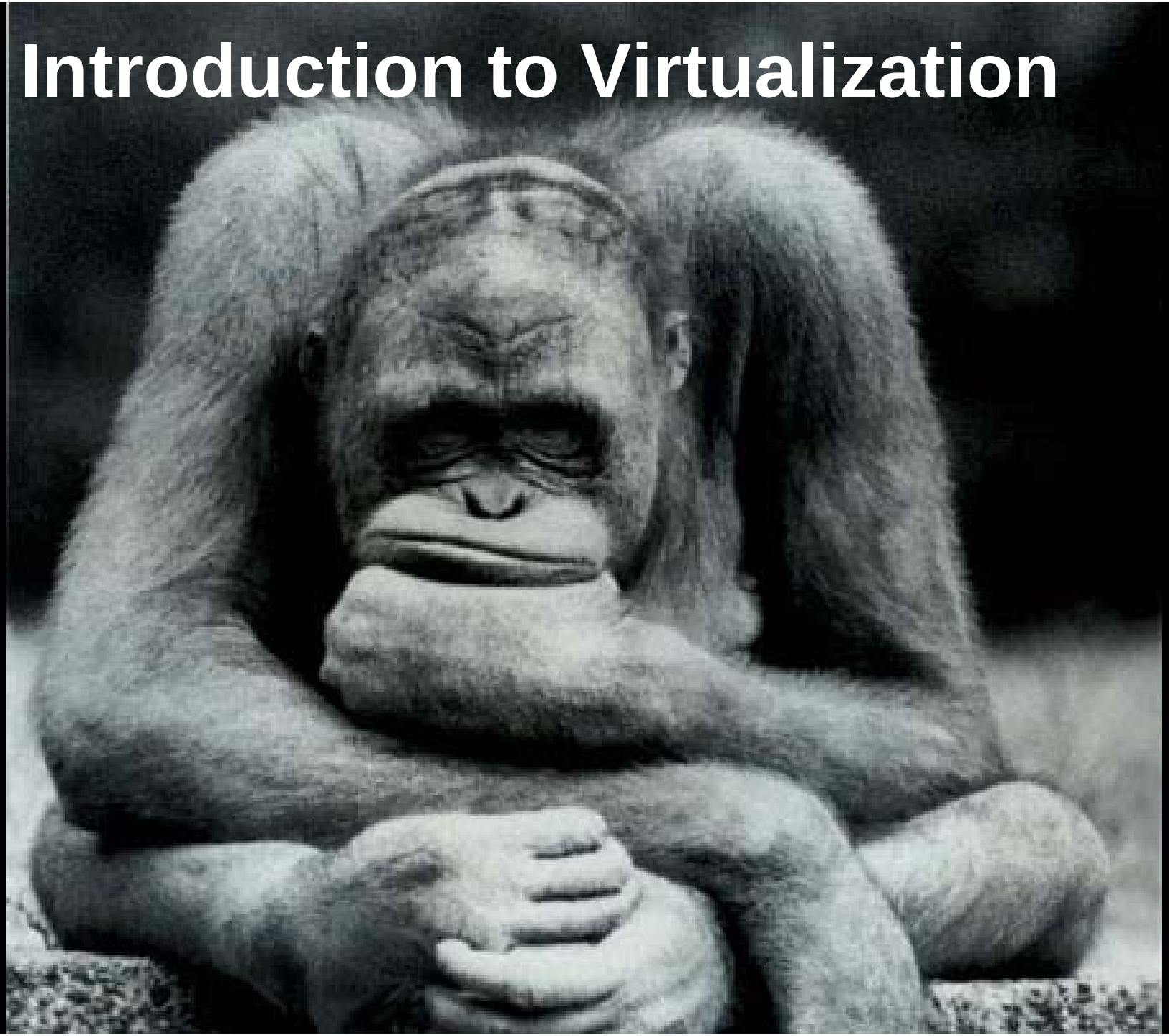
IT Innovation: requiring new ways to secure the new ways we collaborate

The global economy: Fluctuations in economic climates

Flexibility in business methods: to improve operations and serve customers

vb 2008 OTTAWA

Introduction to Virtualization



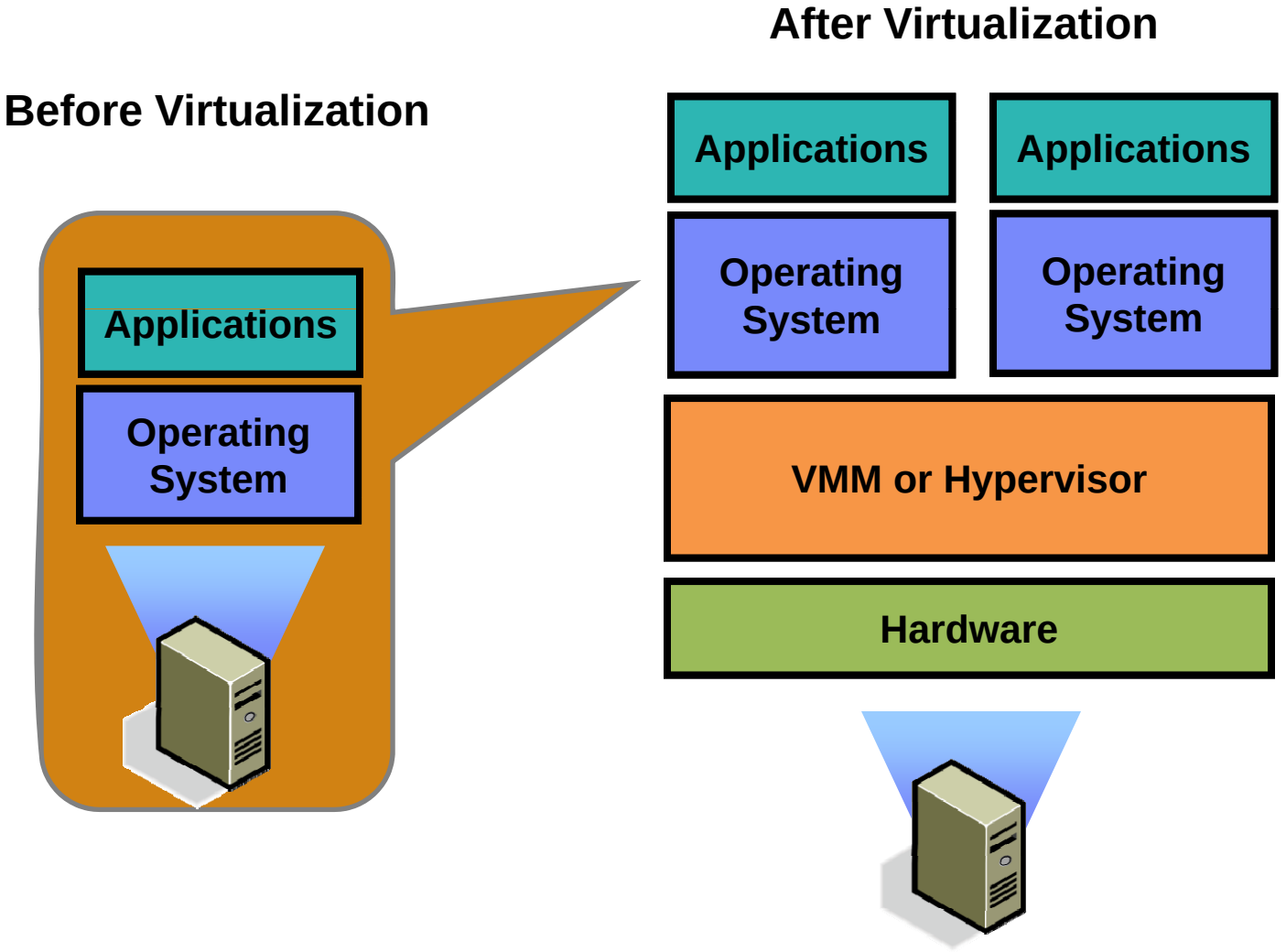
Basics: Disruptive Innovation

Virtualization is a Disruptive Innovation

Virtualization:

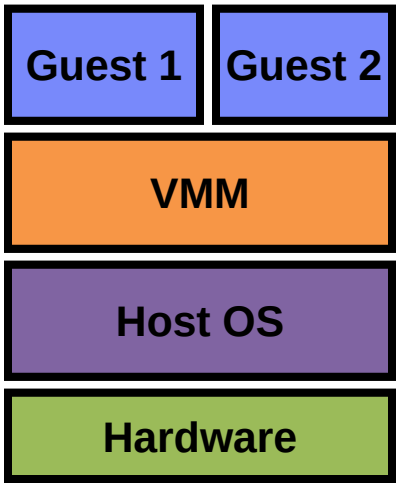
The logical abstraction of physical computing resources (OS, application, switches, storage, networks) designed to create computing environments that are not restricted by physical configuration or implementation.

Basics: Virtualization Architecture



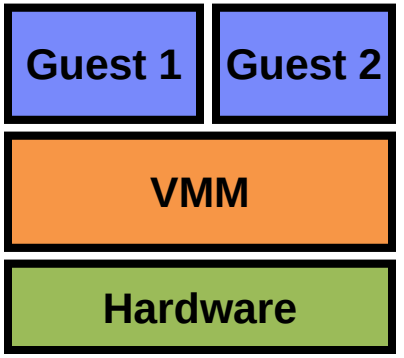
Basics: Virtualization Types

type-2 VMM



Examples:
KVM (Linux)
VMware Workstation
VMware Server
Microsoft Virtual PC

type-1 VMM



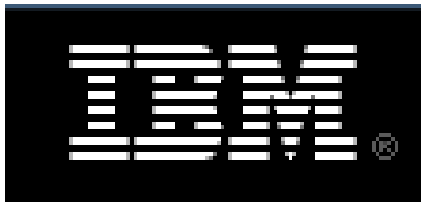
Examples:
Xen
VMware ESX
IBM pHype / LPARs
Microsoft Hyper-V

What does Virtualization Change?

- **Everything**
  - Dynamic, fluid data-center
  - Resource pools
  - Commoditization of everything
  - Increased efficiency
- **Nothing**
  - Virtual IT is still IT
    - Security, sprawl, management, complexity, heterogeneity

Major Players

- Founded in 1998
- Division of EMC



- Pioneered virtualization over 40 years ago
- LPAR, sHype, Phantom

- Acquired XenSource in 2007 for $500 million
- Based on open-source Xen hypervisor

- Virtual server, acquired VirtualPC in 2003 from Connectix
- Hyper-V (fka Viridian) to be released in 2008

- Based on open-source Xen hypervisor

Security and Risk Implications

Virtualization and Enterprise Security

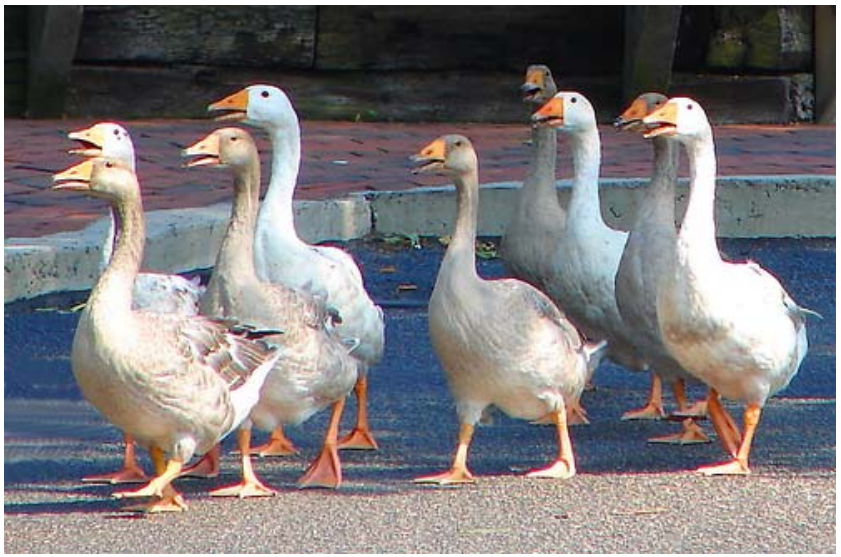
- **Virtualization != Security**
  - Standard servers are as secure as standard VMs
- **Partitioning divides VMs, but does not secure them**
- **Same principles apply**
  - Defense in depth
  - Network design and segmentation
  - Unified security management

Threat Landscape

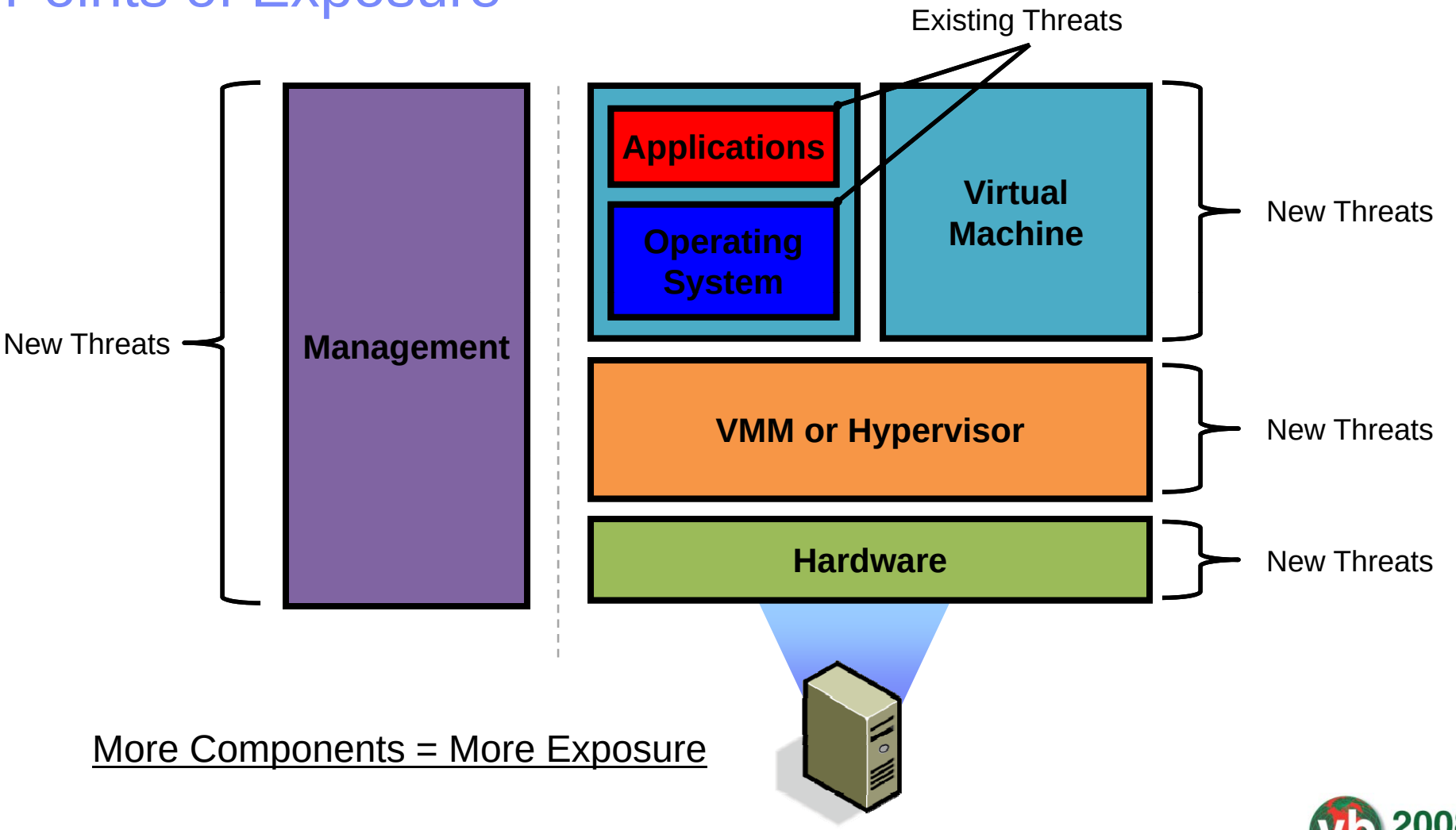
- **New Swath of Availability Attacks**
  - Owning a single guest
  - Breaking out of the guest
  - Compromise of Virtual Console/Management
    - Provision my own evil guest(s)
    - Adjust resource quotas
    - Shut OFF guest(s)
  - Compromise of the VMM/Hypervisor
    - IsGameOver()

Threat Landscape (cont.)

- **Other Threats…**
  - Regulatory
  - Auditors
  - Org-Charts...
    - Separation of Duties
    - Politics

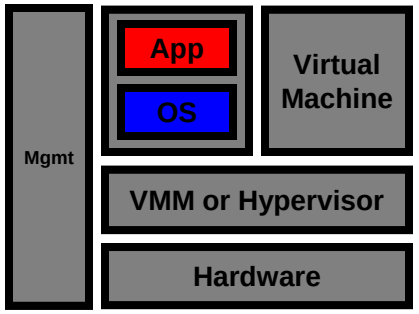


Points of Exposure



More Components = More Exposure

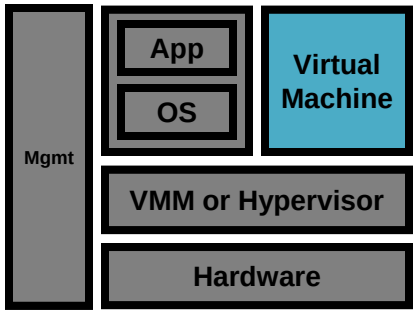
Operating Systems and Applications



- **Traditional threats remain:**
  - Malware: Viruses, Worms, Trojans, Rootkits
  - DoS/DDoS attacks
  - Buffer Overflows, SQL Injection, XSS
  - Data Leakage
  - Access Control, Compliance, Integrity
- **Virtualized OSes and Apps threats remain:**
  - Disaster Recovery and Sandboxing are notable arguments
  - However, they do not increase native resistance to OS/Application threats

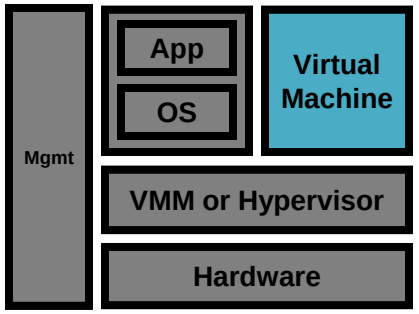
Virtual Machines

- **Compliance and Patching**
  - Ability to “Suspend” / “Activate” VMs alters update lifecycle.
- **Virtual Sprawl and Identification**
  - Difficult to keep track of VMs. Unmanaged, rogue VMs.
- **Dynamic Relocation (Live Migration)**
  - Are VMs moving to less secure machines, networks, datacenters, etc?
  - Static security policies no longer apply.

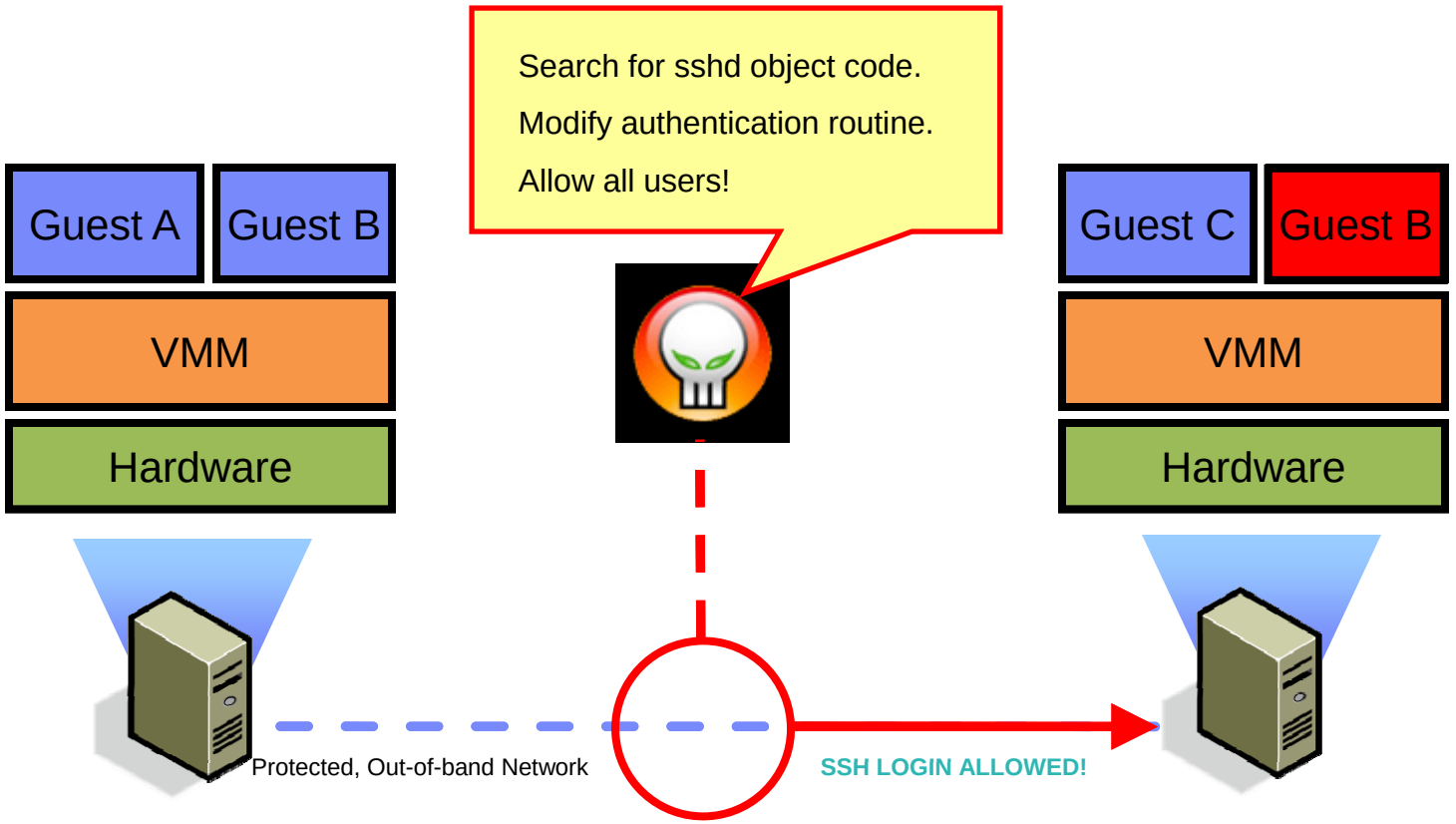


Virtual Machines (cont.)

- **Replay Attacks and Data Retention**
  - VM replay may foster advanced cryptographic attacks.
  - Is sensitive data being cached in unknown areas for replay purposes?
- **Virtual Machine Stealing**
  - VMs are just as files, its trivial to steal a full system or groups of systems.



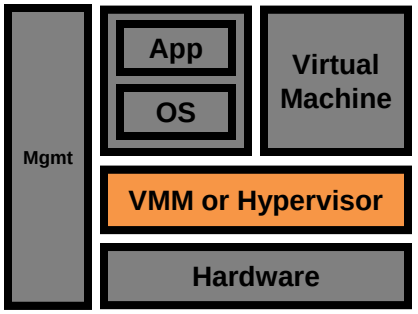
Exploiting Live Migration: Xensploit

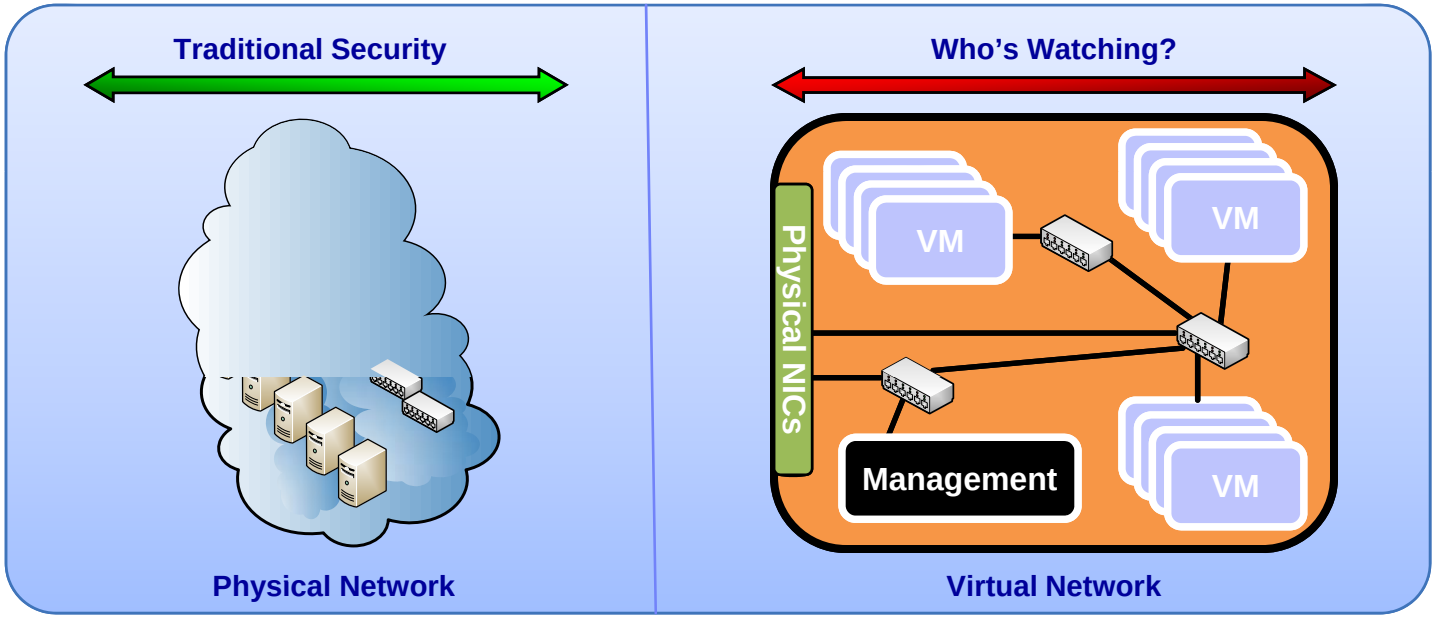


By default, live migration traffic is sent in plain text across the network.
A man-in-the-middle attack can be used to own endpoints in limitless ways.

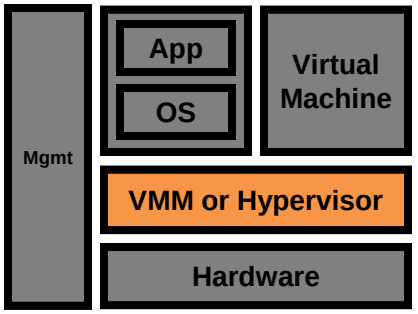
Virtual Machine Manager / Hypervisor

- **Single Point-of-Failure/Attack**
- **Mandatory Access Control / Resource Sharing**
  - Can we guarantee isolation, sharing and communication?
- **Inter-VM Traffic Analysis:**

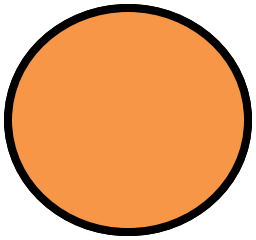




VMM / Hypervisor (cont.)



- **Attacks against the VMM / Hypervisor.**
  - There are going to be bugs that lead to security risks.
  - Shrinking size of VMMs is good for security, but does not make them immune to risk. Features demand complex code.



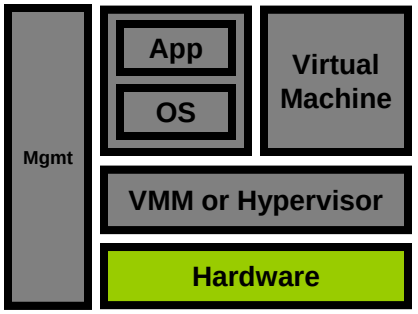
VMware ESX 3
~2GB Surface Area
Lines of Code: Millions

VMware ESX 3i
~32MB Surface Area
Lines of Code: ~200,000

- **Hypervisor Services**
  - Network – DHCP, vSwitching, general packet processing
  - Communication – Inter-domain communication APIs (VMCI, XenSocket)
  - Other Services – Security (VMsafe), Disaster Recovery (vMotion), etc.

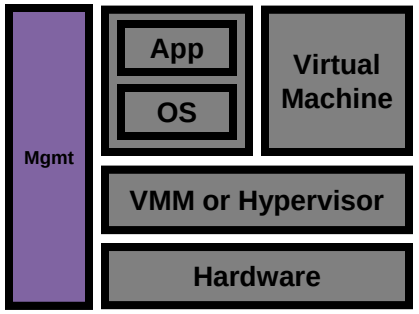
Virtualization-Aware Hardware

- **Hardware Assist (Intel-VT, AMD-V)**
  - Techniques (e.g. rootkits) with stealth capabilities.
  - Low-level makes detection more difficult.
  - Risk to non-virtualized deployments.
    - Blue Pill: Malicious hypervisor injection for AMD-V
    - Vitriol: Leverages Intel VT-x



- **I/O Virtualization**
  - VMs natively share virtualization-aware I/O devices.
    - Virtual Ethernet Cards (vNICs), Virtual FC HBAs (vHBAs), etc.
  - How do we secure a new class of on-demand, dynamic and virtualized allocation of resources?

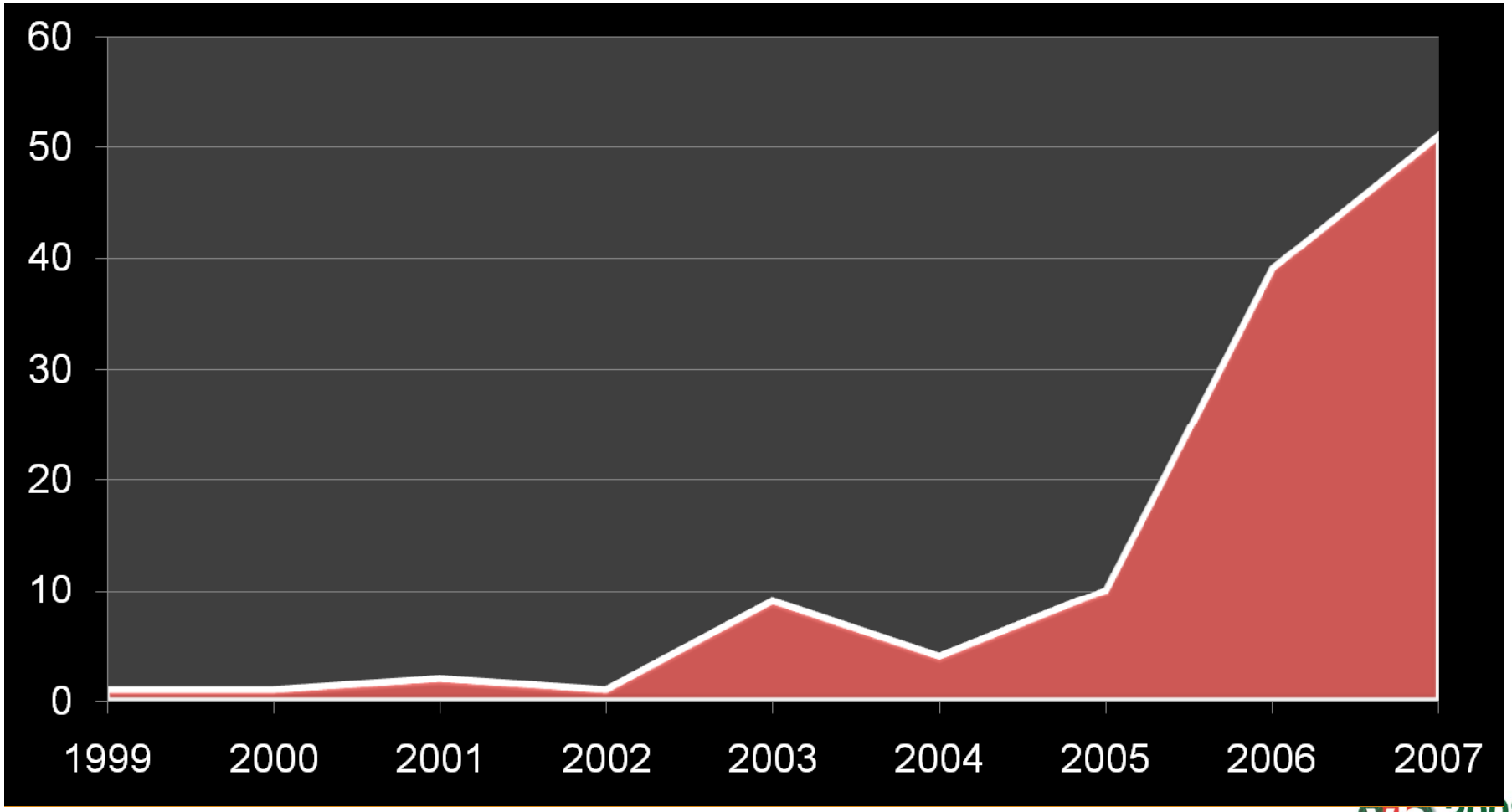
Management Infrastructure



- **Software Threats:**
  - Keys to the castle.
  - Vulnerabilities in management applications.
  - Secure storage of Virtual Machines and management data.
- **Operational Threats:**
  - Managing risk requires new technology, skills and expertise.
  - We now also factor the extremely dynamic nature of virtualization into our evaluation of overall risk.

Vulnerabilities by Year

XFDB Search: VMware, Xen, Virtual PC, QEMU, Parallels, etc.



Operational and Organizational Implications

Organizational Ownership?

- **Who owns the Virtual** [Fill in the Blank] **?**

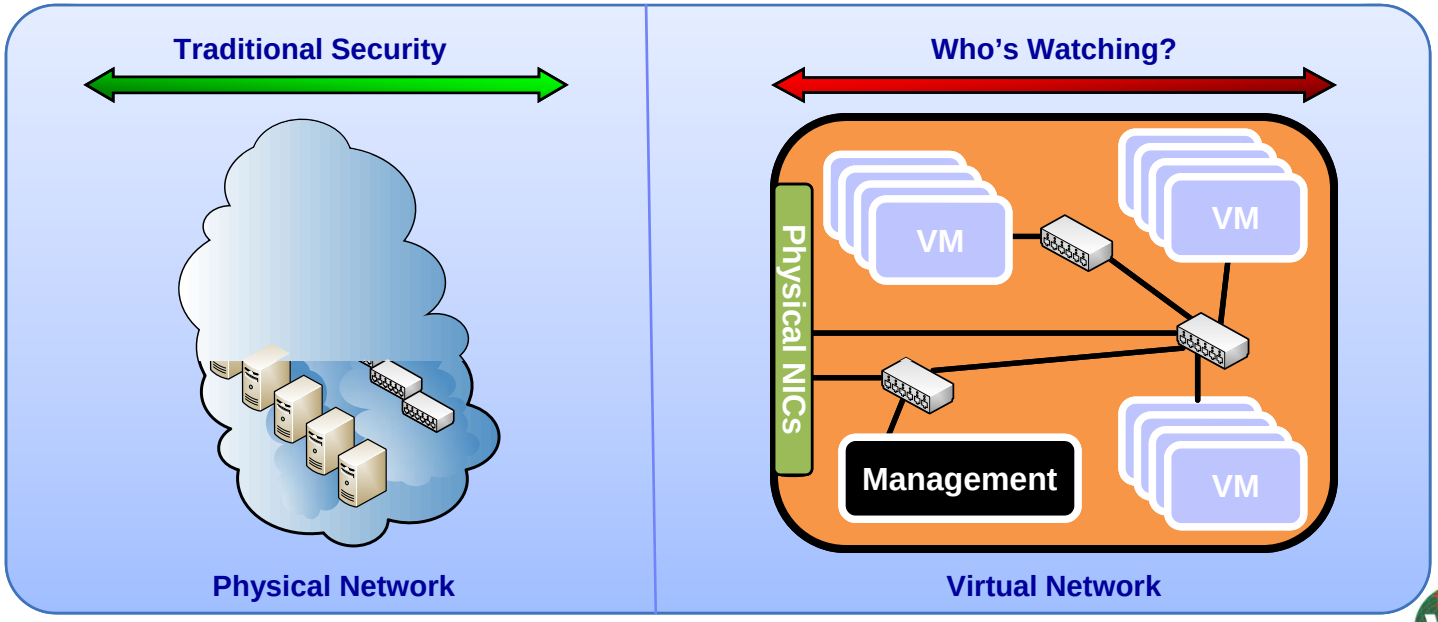
Network Admin

Server Admin

Application Owners

Data Custodians

?



Organizational Ownership?

- **Traditional disciplines and functions still require competence**
- **Separation/Segregation of Duties remains critically important**
- **Care and Feeding of the Virtual Infrastructure will also be required**
  - Are you likely to have a mix of Physical and Virtual Servers?
  - Are you likely to have a heterogeneous mix of Virtual platforms?

Politics of Ownership

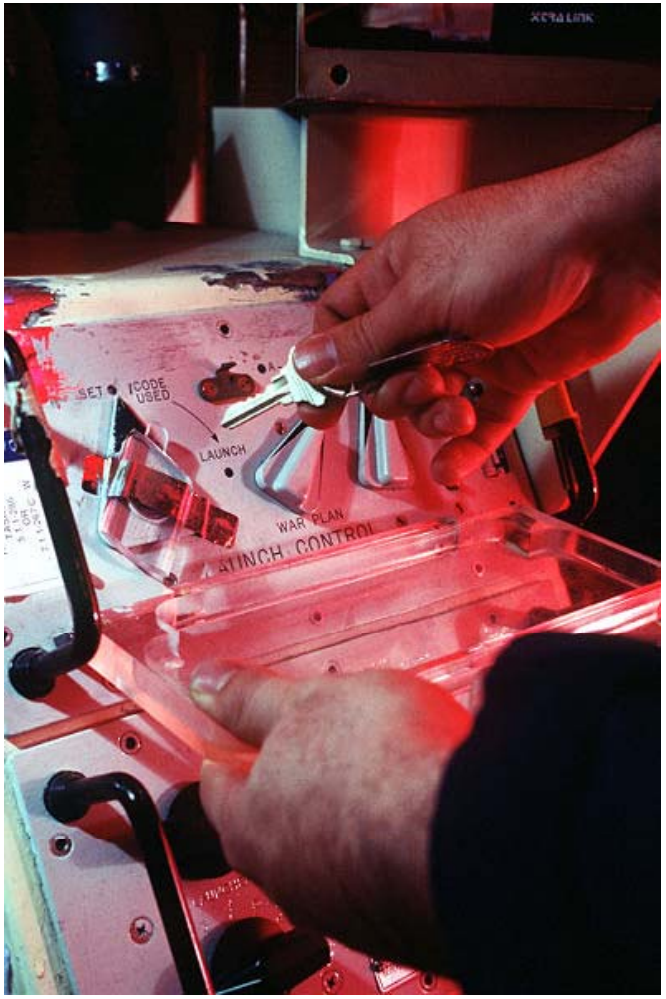
- **“Turf Wars” and “Land Grabs” are possible**
- **“Hot Potato” is also possible**
- **“Finger Pointing” is probable**

New Operational Challenges

- **Find the Server…**
  - Live Migration makes servers harder to track
- **Configuration/Patch Management**
  - Pause/Offline features impact:
    - Audits
    - Scanning
    - Patching
  - Boot Prone?
- **Image Management**
  - Storage
  - Version Control

Operational Controls

- **Discipline, Discipline, Discipline**
- **What are your policies for use of Virtualization?**
  - Which Servers can be clustered?
  - Which Servers cannot be clustered?
- **What are your controls for provisioning?**
  - Easy to slip into Virtual Sprawl
  - Two Key System?



Common Mistakes

Elective Risk

- **Never use Type 2 Server Virtualization for Production**
  - True Story…
- **These “Free” versions of the platform are meant for Testing**
- **Type-2 VMM specific vulnerabilities**

Failure to Establish Policy

Before it gets away from you…

- **Establish Clear Use Guidelines**
- **Establish Clear Roles & Responsibilities**
- **Establish Controls for Provisioning**
- **Establish Intelligent Image Management**
- **Establish Security Guidelines**
- **Establish Compliance Requirements**

Failure to Consider Compliance

- **Will you still be PCI Compliant?**
  - Consult your Auditors **Early and Often**
- **PCI DSS 2.2.1 states:** "Implement only one primary function per server"
  - How does your auditor interpret this?
  - What I've seen…
- **Anticipate Future Regulatory Granularity**
  - Right now Virtualization is ahead of Compliance

Failure to Involve Security

- **By default, Virtualization reduces your security posture**
  - New attack surfaces
  - New operational risks
  - New availability risks
  - Increased complexity that comes with beneficial features
    - E.g. Live Migration
- **Security Analysis/Design can inform smart compensating controls and best practices while countermeasures mature**

Failure to Control Live Migration

- **Cascading Failover Example**
  - True Story…
- **We often overlook the fluid realities of Live Migration**
  - E.g VMotion

“Silver Bullet” Virtual Appliances

- **Today’s Virtual Security Appliances are very nascent**
  - Coverage is limited
  - There is NO Silver Bullet
  - Buzz Words and Snake Oil abound
  - Realistic expectations can help reduce over-confidence in these products
- **Security will improve as Virtual Platforms release their Security APIs and as Security Vendors leverage them**

What Can I Do?

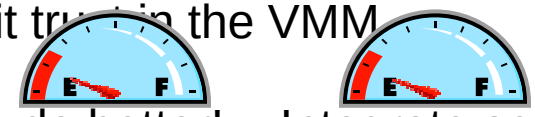
Securing Virtualization: Today

First Generation Virtualization Security:

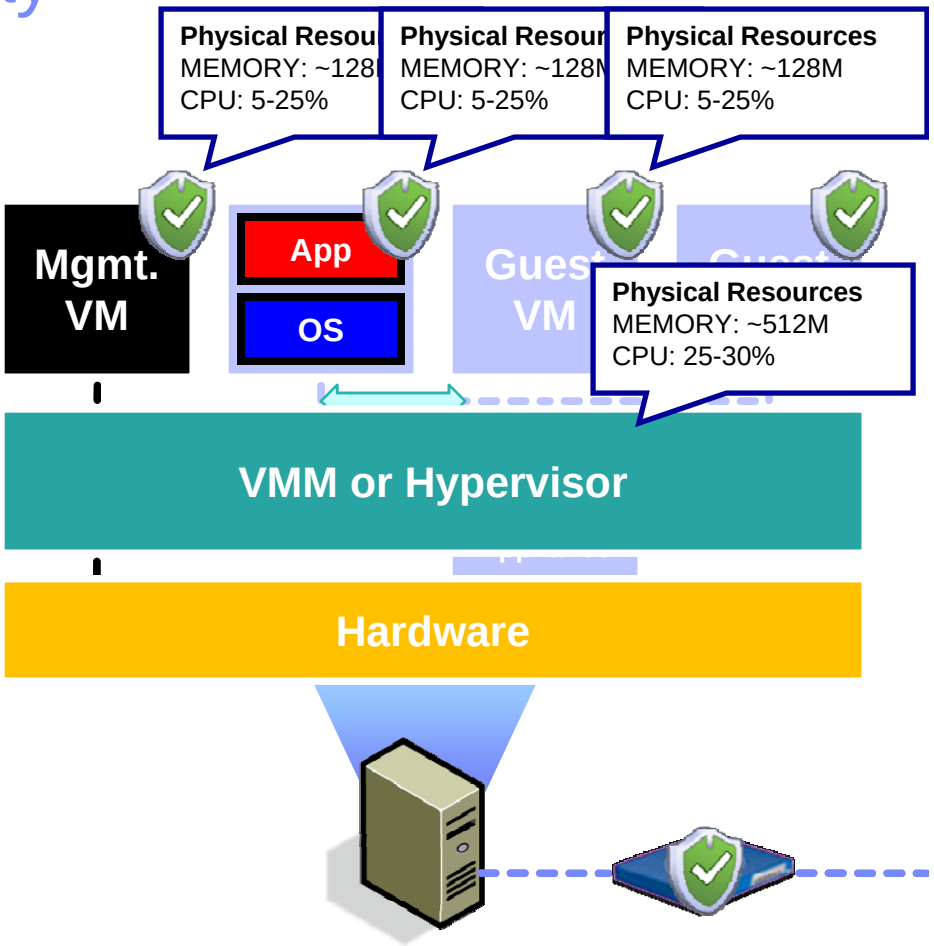
- Install security in each guest VM.
- Apply defense-in-depth.
- Lock-Down Management.
- Segment networks with VLANs.
- Use stand-alone security appliances.

Potential Limitations:

- New VMs need security provisioning.
- Redundant security = more resources.
- Management nightmare.
- Inter-VM network traffic analysis.
- Implicit trust in the VMM



We can do better! - Integrate security into the Virtual infrastructure, don't bolt it on.



Securing Virtualization: Tomorrow

Next Generation Virtualization Security:

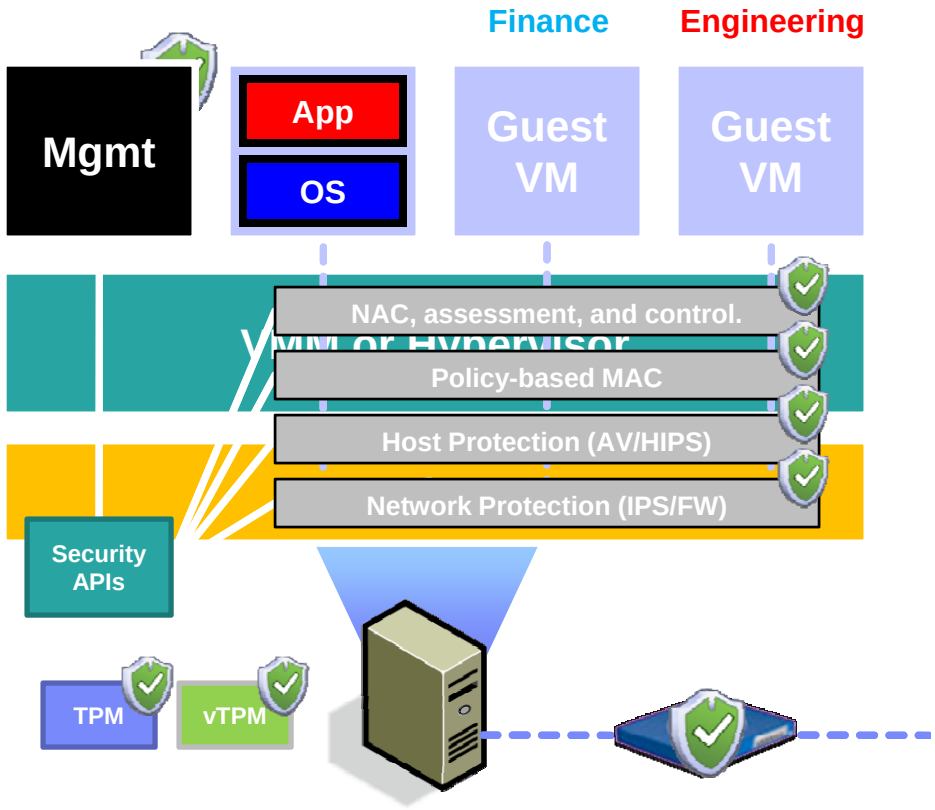
- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

Security VM Features:

- Centralized network protection.
- Agent-less host protection.
- Policy-based MAC and isolation.
- VM NAC, assessment, and control.

Additional Security:

- Hypervisor attestation (TPM)
- VM attestation (vTPM)



Gunter Ollmann – *Chief Security Strategist*
IBM Internet Security Systems
gollmann@us.ibm.com
http://blogs.iss.net

Questions?

Further Reading

- **Chris Hoff's BLOG "Rational Survivability"**
  - http://rationalsecurity.typepad.com/blog/
  - http://rationalsecurity.typepad.com/blog/virtualization/index.html
  - Ongoing Virtualization Thought Leadership
- **Neil MacDonald of Gartner**
  - Several Excellent Research Notes
- **X-Force Threat Research**
  - http://www.iss.net/x-force_threat_insight_monthly/index.html
  - http://blogs.iss.net/
- **Center for Internet Security Benchmarking**
  - http://www.cisecurity.org/bench_vm.html