IBM Global Services

Virtualization != Security

Dan Ingevaldson
Manager, Technology Strategy
IBM Internet Security Systems

IBM Internet Security Systems
Ahead of the threat.™

Virtualization Market Update

Virtualization Trends

- Gartner predicts that virtualization will be the **most impactful** trend in IT infrastructure and operations through 2010.
- IDC estimates **1 million** virtualized server footprints by 2009**, $15B** in hardware revenue.
- **70%** of large organizations will collapse all or part of their DMZ by using risk-managed virtualization techniques by 2010.[3]
- Primary drivers of server virtualization adoption[4]:
  - Reducing infrastructure costs (server consolidation).
  - Enabling easier and more flexible application deployment.
  - Improving server utilization rates.

Gartner

FORRESTER

YANKEE GROUP

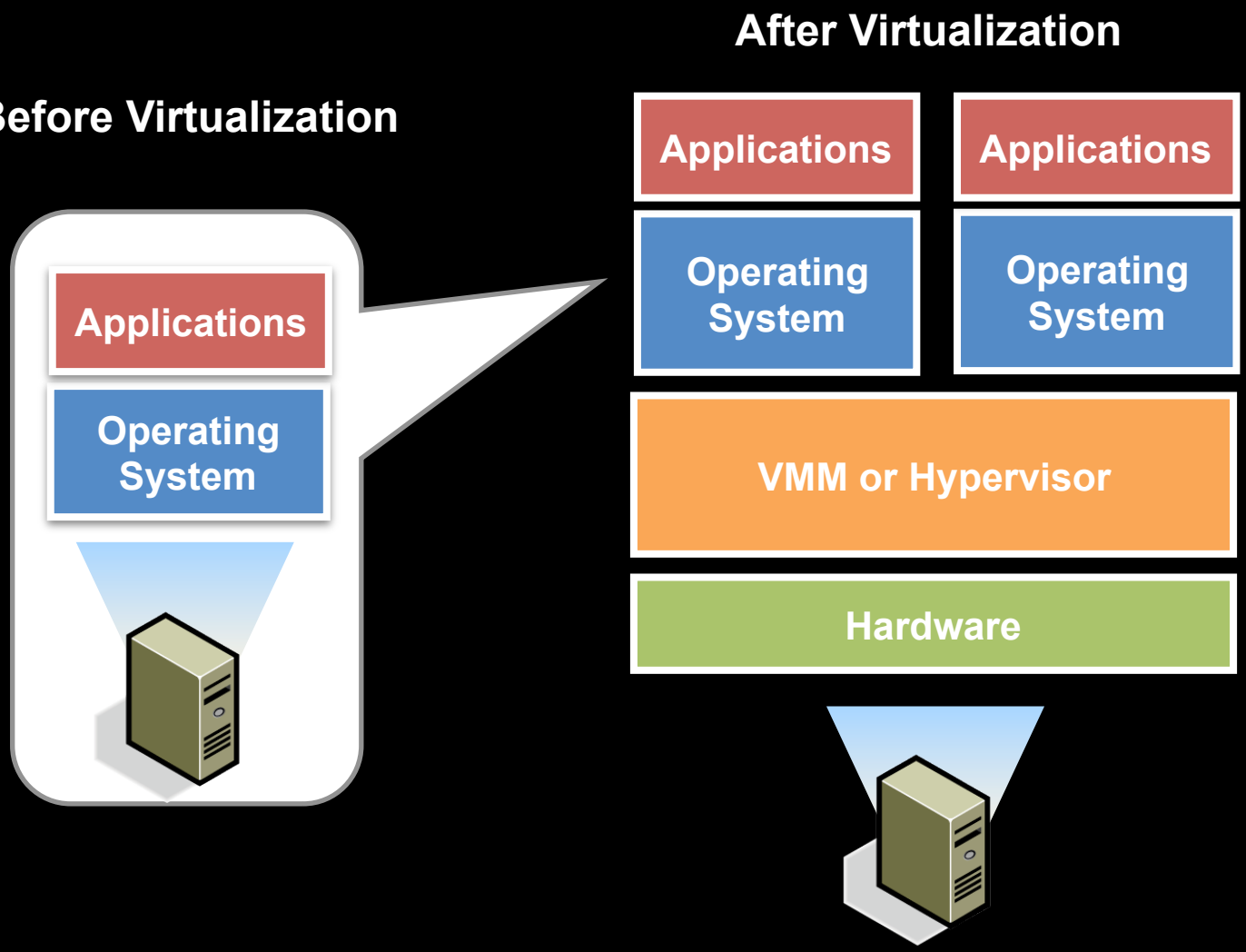
[1] Forrester Research: "System Management For a Virtualized World" July 10, 2006

[2] Yankee Group: "Virtualization, Part 1: Technology Goes Mainstream, Nets Corporations Big TCO Gains and Fast ROI" July 2006

[3] Gartner: "Server Virtualization Can Break DMZ Security" May 24, 2007

[4] Yankee Group: "Virtualization, Part 2:Server Virtualization is Transforming Enterprise IT" August 2006

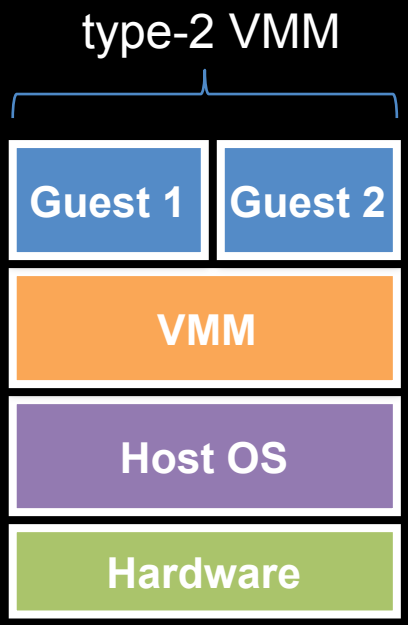
Basics: Virtualization Architecture



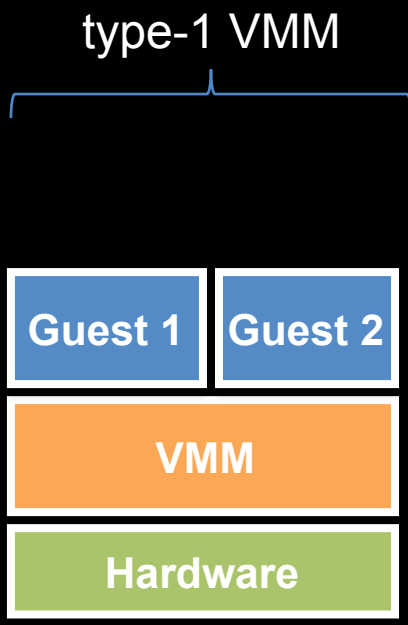
Virtualization != Security– PART I

TRENDS, BASICS, THREATS

Basics: Virtualization Types

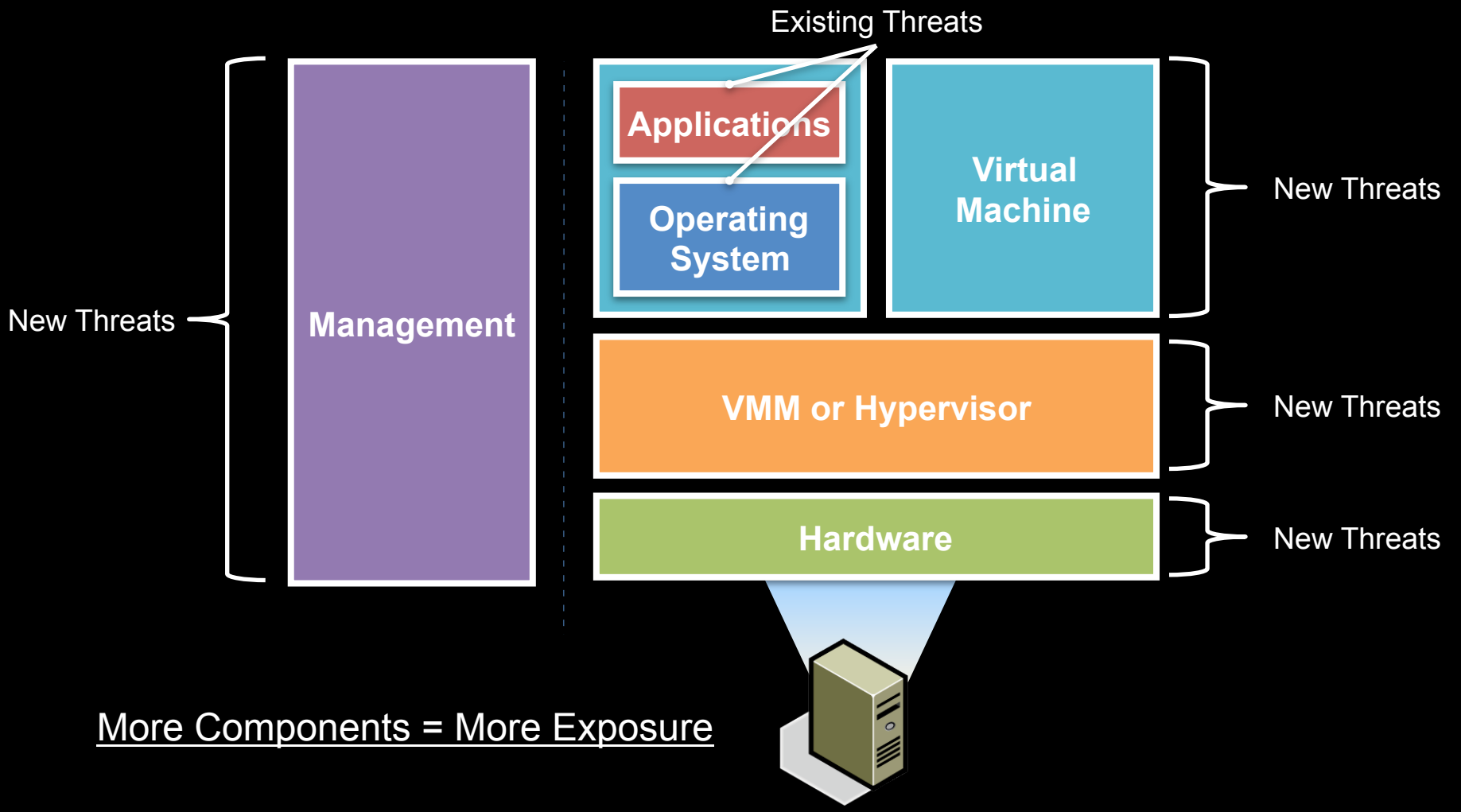


Examples:
KVM (Linux)
VMware Workstation
VMware Server
Microsoft Virtual PC



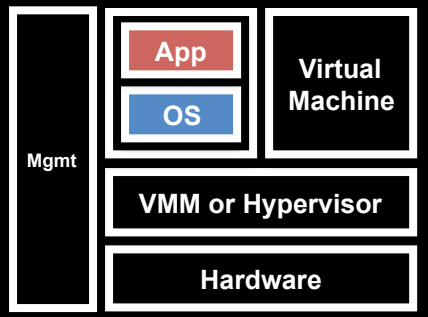
Examples:
Xen
VMware ESX
IBM pHype / LPARs
Microsoft Hyper-V

Threat Landscape



More Components = More Exposure

Operating Systems and Applications



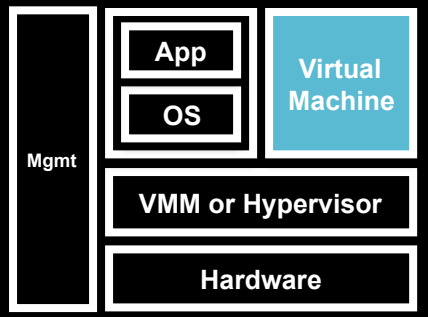
Traditional threats remain:

- Malware: Viruses, Worms, Trojans, Rootkits
- DoS/DDoS attacks
- Buffer Overflows, SQL Injection, XSS
- Data Leakage
- Access Control, Compliance, Integrity

Virtualized OSes and Apps are not more secure… yet…

- 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.

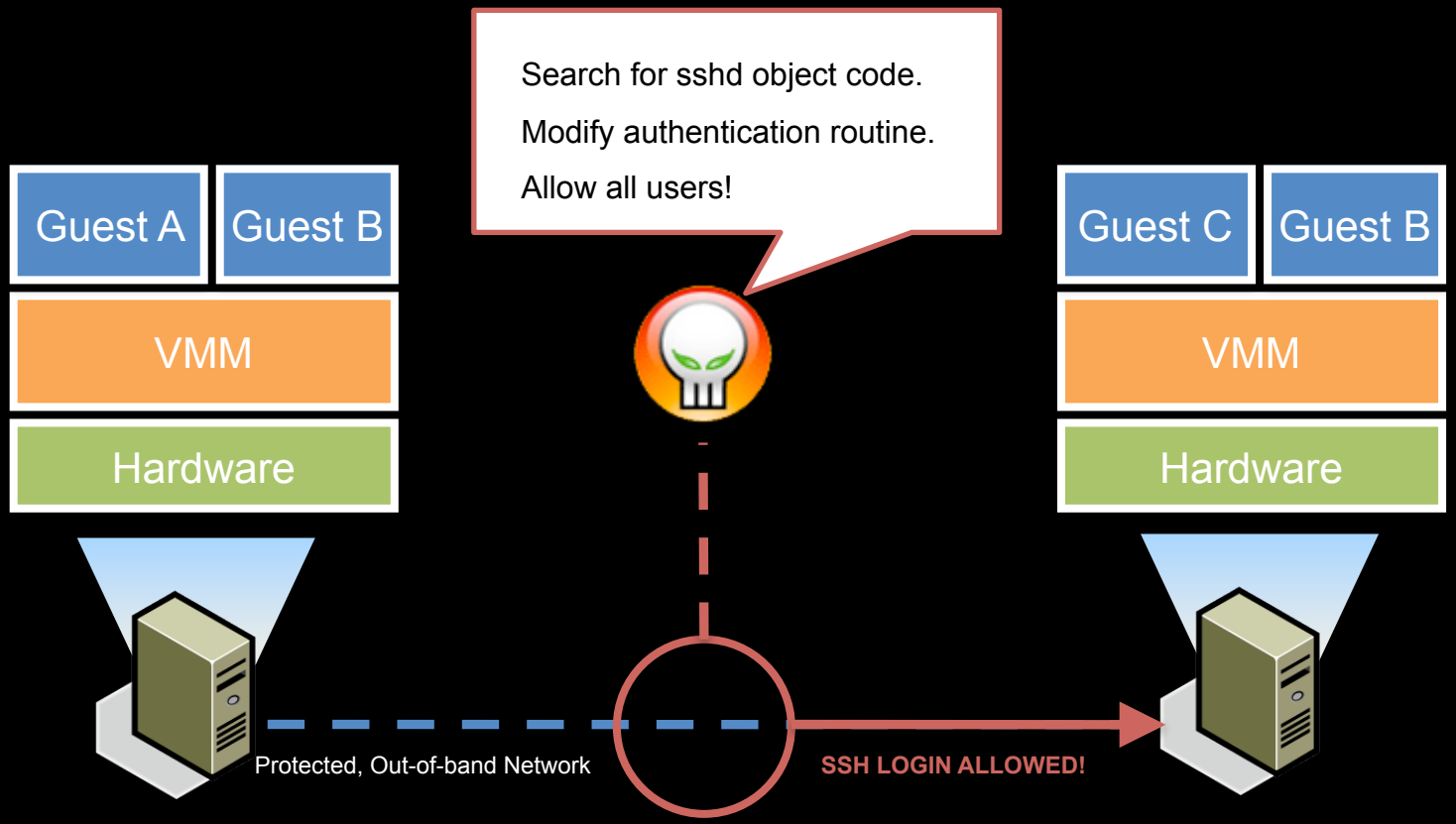
Replay Attacks and Data Retention

- VM replay may foster advanced cryptographic attacks.
- Is sensitive data being cached in unknown areas for replay purposes?

Virtual Machine Stealing

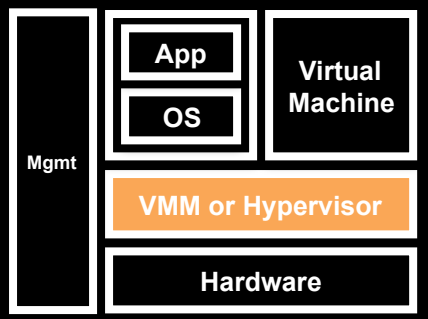
- VMs are just files, its trivial to steal a full system or groups of systems.

Exploiting Live Migration: Xensploit



A Bydefault, live migration traffic is sent in plaintext across the network.

Virtual Machine Manager / Hypervisor

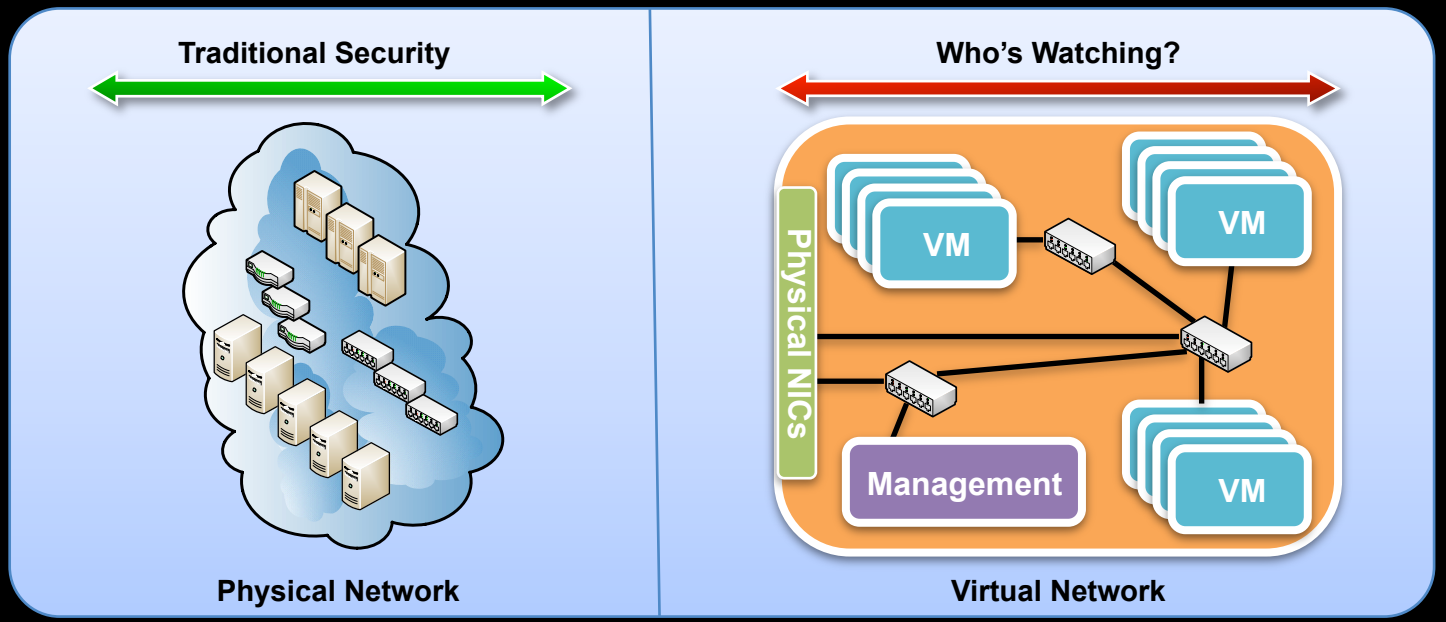


Single Point-of-Failure, Point-of-Attack

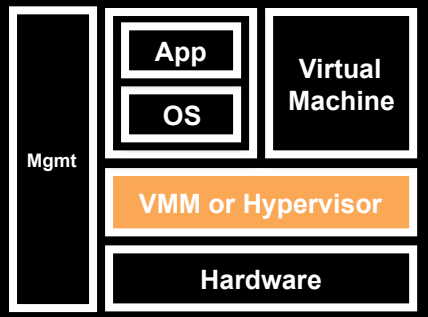
Mandatory Access Control / Resource Sharing

- Can we guarantee isolation, sharing and communication?

Inter-VM Traffic Analysis:

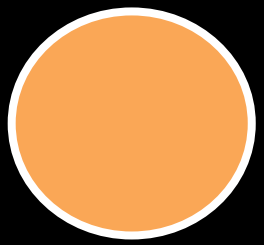


Virtual Machine Manager / Hypervisor (cont.)



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.



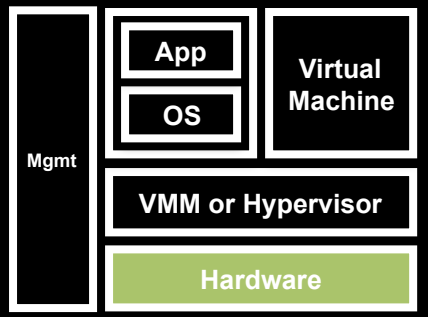
VMware ESX 3
~2GB Surface Area
Lines of Code: Millions

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



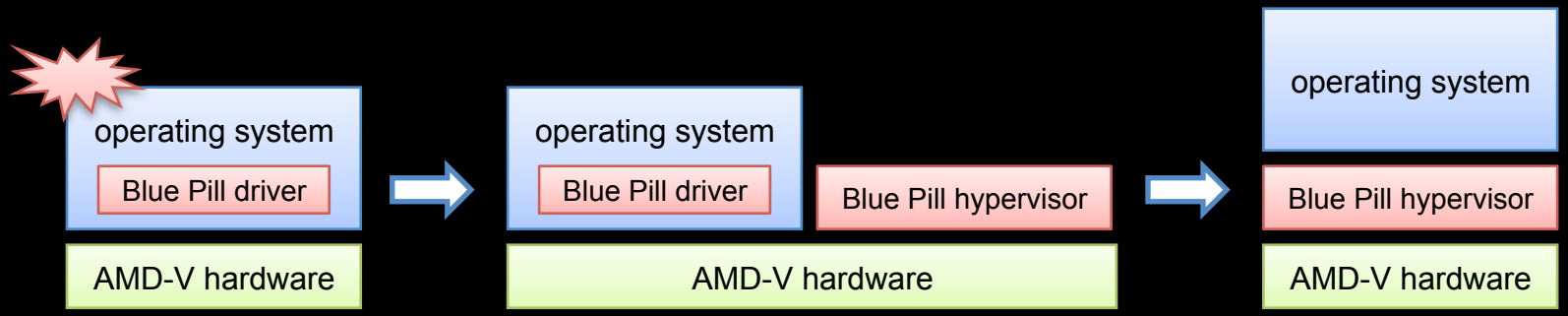
Hardware Assist (Intel-VT, AMD-V)

- Techniques (e.g. rootkits) with stealth capabilities.
- Low-level makes detection more difficult.
- Risk to non-virtualized deployments.
  - Blue Pill: Malicious hypervisor injection on machines not using hardware capabilities.

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?

HVM-based Rootkits: Blue Pill



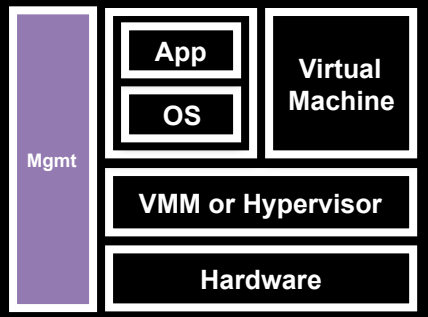
Blue Pill exploits the OS and inserts a malicious driver into the kernel.

The driver enables SVM, sets up the VMCB, and loads the Blue Pill hypervisor into memory. Execution is transferred to the hypervisor and VMRUN is called.

The OS now runs in a VM. Execution is transferred back to the driver for removal.

- Blue Pill requires hardware-enabled machines not running virtualization.
- Blue Pill exploits Operating System / Software bugs to install.
- **New research aims to accommodate nested virtualization.**

Management Infrastructure



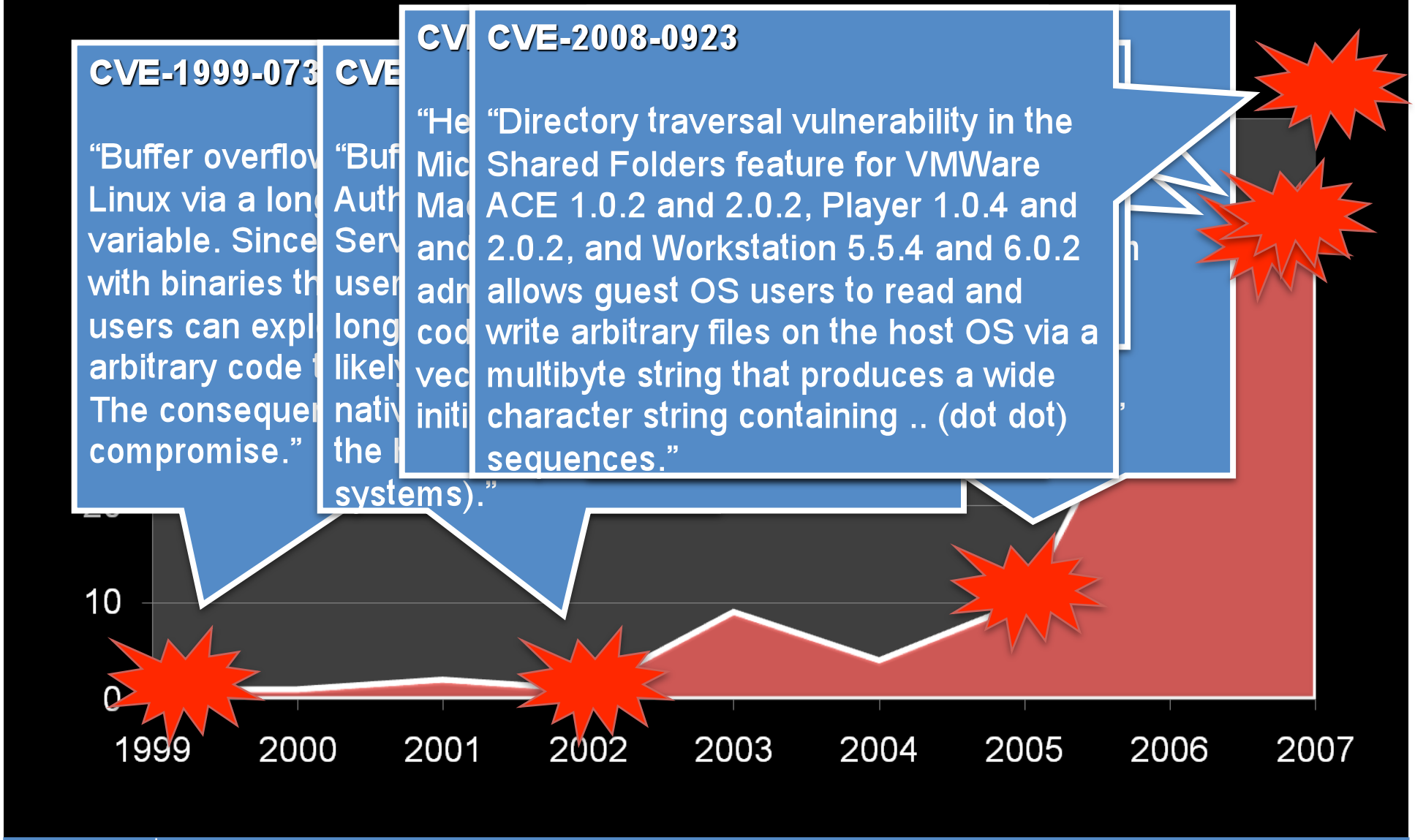
Software Threats:

- 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



Virtualization != Security – PART II

SECURING VIRTUALIZATION

Virtualization Protection Solutions

Virtualization Security has many attributes:

- Virtual security services vs. securing the platform vs. securing VMs.

Securing VMs requires unique capabilities.

- Future solutons should offer the granularity, visibility, correlation and scalability required to properly secure virtual machine deployments.

Bake-in the security.

- Create solutions specifically for virtualization and integrate this security into the platform.

How do we get there?

Beyond virtual form-factor solutions

- Significant management overhead as virtual network complexity increases.
  - exponentially when inter-VM communication must be protected

Integrated and automated solutions

- Find optimal analysis points to reduce redundancy and overhead.
- Automate discovery and security provisioning.
- Partner with virtualization platform vendors.
- Use the VMM to understand/modify VMs and their I/O.
  - Alter and inspect VM network, disk, memory, and cpu state.
- Components and libraries: VMsafe, XenAccess, sHype, vTPM.

More attributes of virtual security

Minimal footprint and impact on performance

- Guest OS presence include on necessary components.

Transparency throughout fail-over and migration solutions

- Solutions must be as dynamic as the virtual environment.
  - security follows virtual machines (e.g. VMotion)

Multiple layers (Defense-in-depth)

- Risk mitigation solution combines compliance, data security and threat mitigation.

Combination of intelligent analysis and access control

- Both a “good guys in” and “bad guys out” solution.

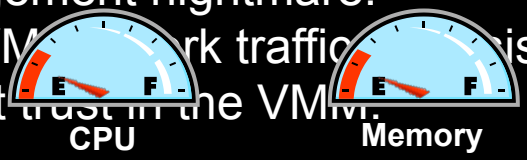
Securing Virtualization: Today

First Generation Virtualization Security:

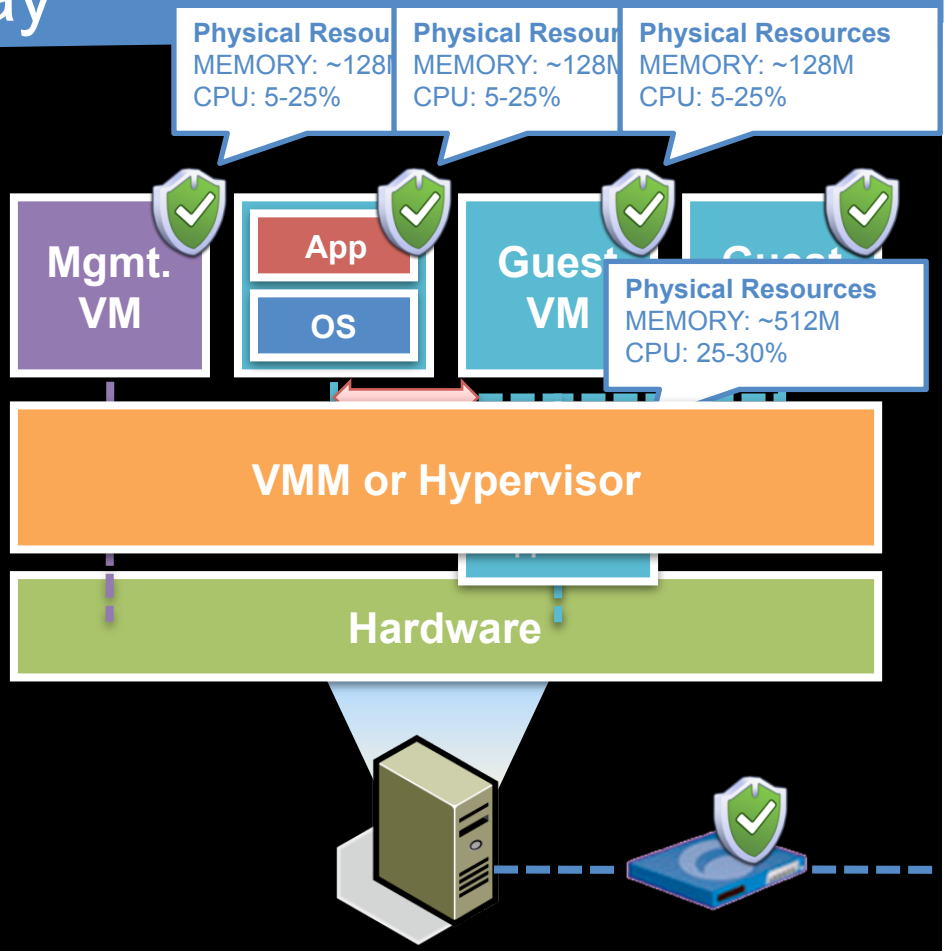
- Install security in each guest VM.
- Apply defense-in-depth.
- Lock-Down Management.
- Segment networks with VLANs.
- Use stand-alone security appliances.

Potential Limitations:

- New VMs need security provisioning.
- Redundant security = more resources.
- Management nightmare.
- Inter-VM network traffic is.
- 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:

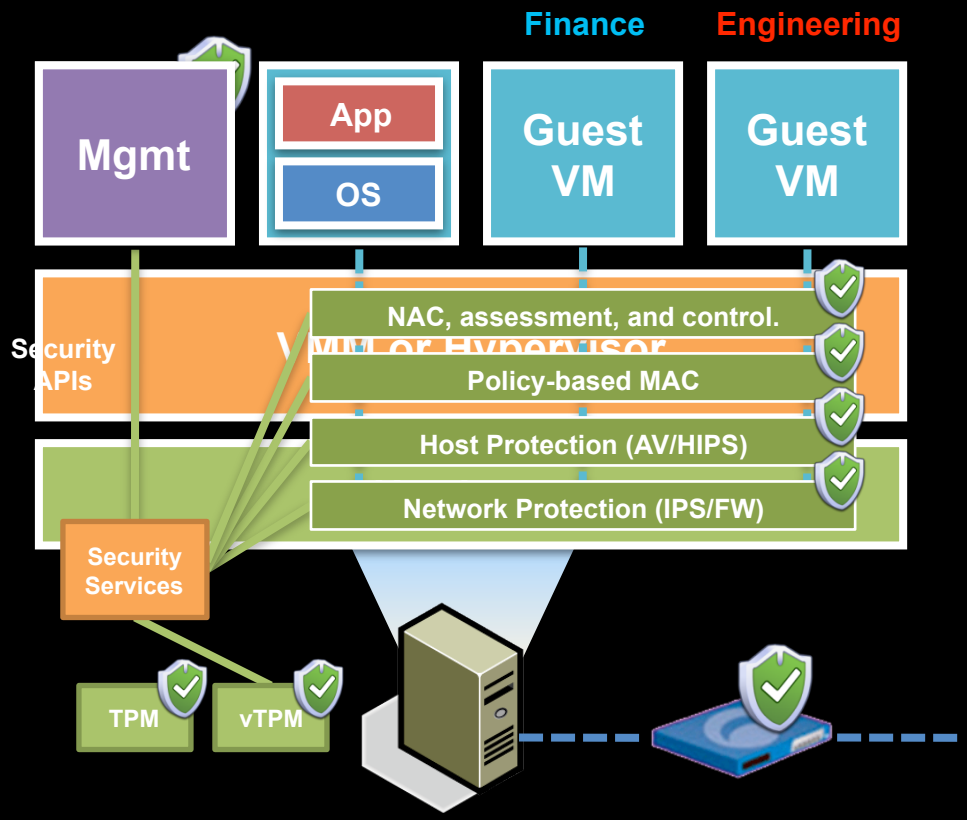
- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

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)



Virtualization != Security – PART III

TAKE AWAYS

Threat Landscape

Virtualization introduces significant technolgical and operational risks. It also changes and/or intensifies old risk.

Virtualization platforms will become the target of choice of the research community/hacker community in the years to come.

The popularity, complexity, and immaturity of x86 virtualization make it very likely that new hypervisor-compromising malware, attacks on management infrastructure, and other malicious activity will make headlines very soon.

Protecting Virtualization

Virtualization security research will be focused on solving these three problems, in this order: isolation, inspection/ protection, and integrity.

Virtual machines have the theoretical ability to be made more secure than their traditional physical machine counterparts.

Physical security solutions, such as "network protection" appliances, become less relevant in a highly virtualization environment - and these devices will begin to take on different roles.

Questions?

THANK YOU!