Better Security with Virtual Machines

VMware Security Seminar
Cambridge, 2006
Agenda

VMware Evolution
  • Virtual machine
  • Server architecture
  • Virtual infrastructure

Looking forward
  • VMware’s security vision

Emerging opportunities
  • Better security with virtual machine
VMware’s Evolution
Virtual Machine Benefits

**Partitioning** – Multiple application and OS instances in a single machine

**Isolation** – Each virtual machine is isolated from the host and other virtual machines

**Encapsulation** – Each entire virtual machine state is contained in software; standard virtual hardware guarantees compatibility.
VMware Evolution

From desktop to server
ESX server architecture

Customized hypervisor kernel
Fast I/O virtualization
Advanced resource scheduler tailored for running VMs
VMware Evolution

Virtual infrastructure
VMware’s Virtual Infrastructure
Distributed Resource Scheduling

Global scheduler

- Automates initial virtual machine placement
- Uses VMotion to continuously optimize based on current workload
- Reacts to adding or removing hosts from the cluster
VMware Consolidated Backup

Transparent to virtual machines
Backup offloaded to dedicated servers
Preserve file level consistency
Integrated with popular backup utilities
VMware Evolution

What’s Next?

VMware Evolution

- Virtual machine
- Server architecture
- Virtual infrastructure

Looking forward

- VMware’s security vision

Emerging opportunities

- Better security with virtual machine
Very Autonomic Security Technology

Automation
- Self -troubleshooting, -repairing, -defending
- Repeatable, reliable, and predictable

Intelligence
- Correlate large amounts of data and learn from data
- Take immediate, accurate action on data

Ubiquity
- More coverage increases accuracy
- Work with heterogeneous environments

VAST provides accurate, ubiquitous protection of virtual machines by automating the process of deployment and operational aspects of information security tasks.
IDC Feb 2005 Worldwide Spending on Security

- Secure content management: 42%
- Identity and access management: 25%
- Security and vulnerability management: 15%
- Firewall/VPN: 10%
- Intrusion detection and prevention: 4%
- Other security: 4%

WW SW Total = $9.8 billion
Agenda

VMware Evolution
- Virtual machine
- Server architecture
- Virtual infrastructure

Looking forward
- VMware’s security vision

Emerging opportunities
- Better security with virtual machine
Emerging Opportunities

Secure Virtual Machines
— trust, automation, intelligence

- Embedded IDS
- Network Interposition
- Attack-Resistant Virtual Hardware
- VM Recovery
Embedded IDS

Use virtualization layer to inspect VM

Unlike traditional system inside VM

Leverages tech trends: Multicore
Network Interposition

VMM can interpose to enhance security

**GOAL:** Only safe and correct communication

Attacks are **dropped** or **contained**
Modify virtual hardware to:
- detect attacks
- prevent attacks
VM Recovery

Use a rollback and replay of VM execution

Forensics
Detect techniques of attack

Attack Recovery
Remove intrusion damage/backdoors from VM
Trust in Virtual

Is software trustworthy?
  • Existing OS environment

Lock trust in hardware
  • TPM
    • Still need software layers

Trust in Virtual Machine
  • VMM layer as security base
  • Virtual TPM and more
  • Application Model
Conclusion

Looking forward

• Security layer out of the OS
• VMM layer as trusted base for security

Virtual even better than real

• Trustworthy
• Autonomic
• Intelligent