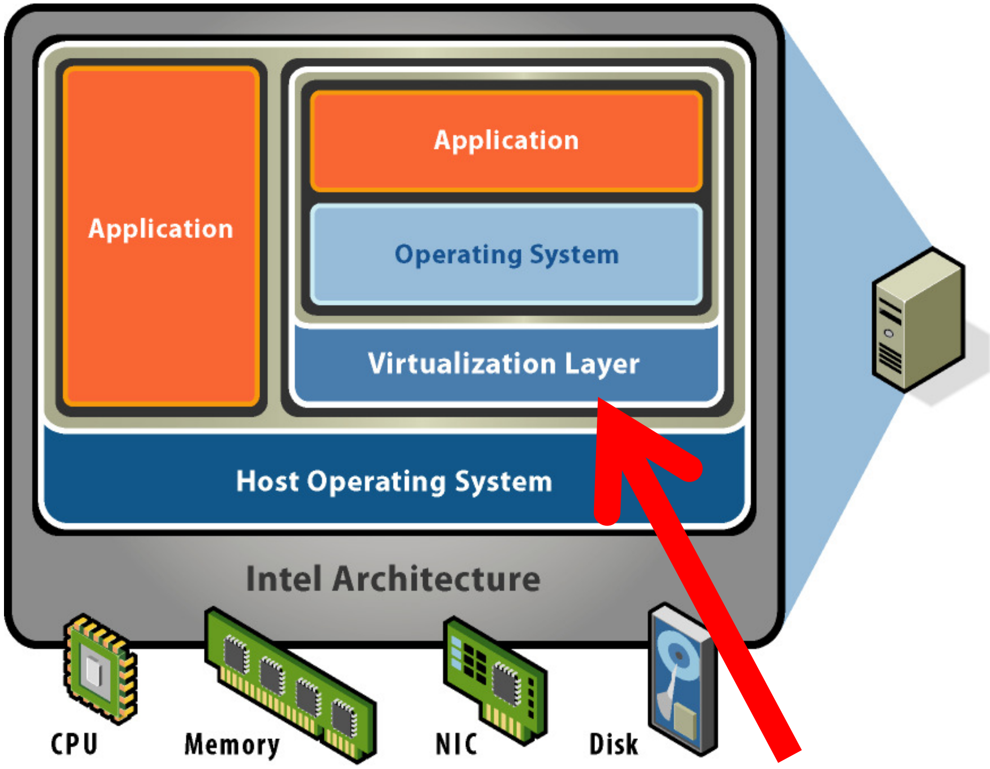
VMware Security Briefing

Steven Boesel, CISSP

Senior Systems Engineer

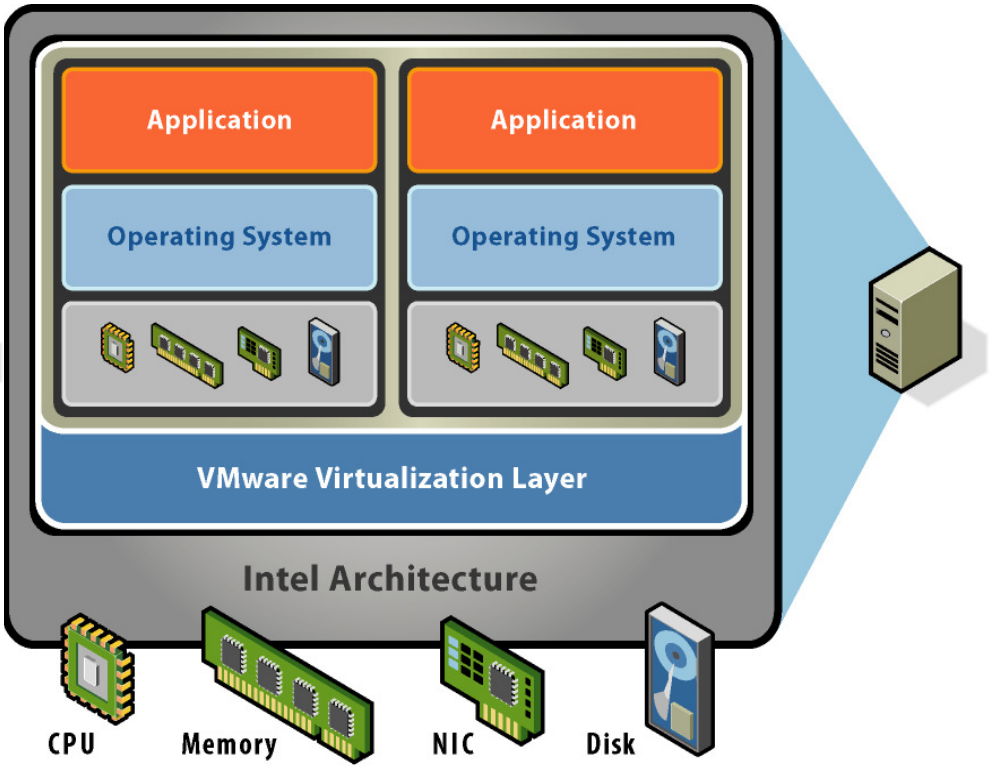
Hosted Virtualization vs. Bare Metal Virtualization

Hosted Virtualization



VMware Workstation
VMware Server
VMware Player

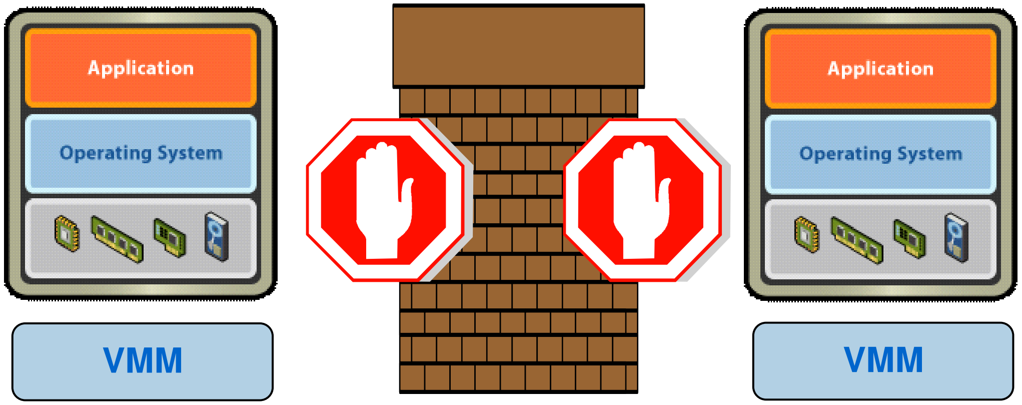
Bare-Metal Virtualization



VMware ESX Server

Host OS Changes
Security Profile Greatly

VMware Architecture: Isolation and Containment



Security Design Highlights

- Privileged instructions within a VM are “de-privileged” and run within an isolated virtual memory space
- VMs have no direct access to hardware, only have visibility to virtual devices
- VMs can only communicate with each other through Virtual Switches
- Resource reservations and limits guarantees performance isolation
- OS and applications within a VM run as is with no modification (hence no recertification required)

Production Use Proof Points

- CC EAL 4+ certification
  - ESX 3.0.2 and VC 2.0.2
- Passed security audit and put into production by the largest Financial Institutions
- Passed Defense and Security Agencies scrutiny and audit (NetTop and HAP)
- Large number of customers run mission critical and transaction processing applications

Are there any Hypervisor Attack Vectors?

There are currently no known hypervisor attack vectors to date that have lead to “VM Escape”

- Architectural Vulnerability
  - Designed specifically with Isolation in Mind
- Software Vulnerability
  - Possible like with any code written by humans
  - Small Code Footprint of Hypervisor (~32MB) Makes it Easier to Audit
  - Depends on VMware Security Response and Patching
  - If a software vulnerability is found, exploit difficulty will be very high
- Commonly cited: Blue Pill, SubVirt
  - These are NOT hypervisor vulnerabilities,
  - Use the concept of a hypervisor to create advanced malware
  - These can only affect non-virtualized operating systems

Common Misconception about VMware Security

Hosted Platforms Guest Escape Vulnerabilities

- **Does NOT affect ESX** only hosted platforms (Workstation and Server)
- Not exactly escape nor a hypervisor vulnerability
- Uses documented communication interface for “hosted” features such as drag-n-drop, cut –n-paste, and shared folders.
- This communication interface can be disabled (on by default)

Security Advantages of Virtualization

- Better Forensics Capabilities
- Faster Recovery After an Attack
- Patching is Safer and More Effective
- Better Control Over Desktop Resources
- More Cost Effective Security Devices

Operational Security Issues

- Adapt existing security processes
- Adapt existing security solutions
- The datacenter becomes much more dynamic and flexible
- Misconfiguration is #1 Risk

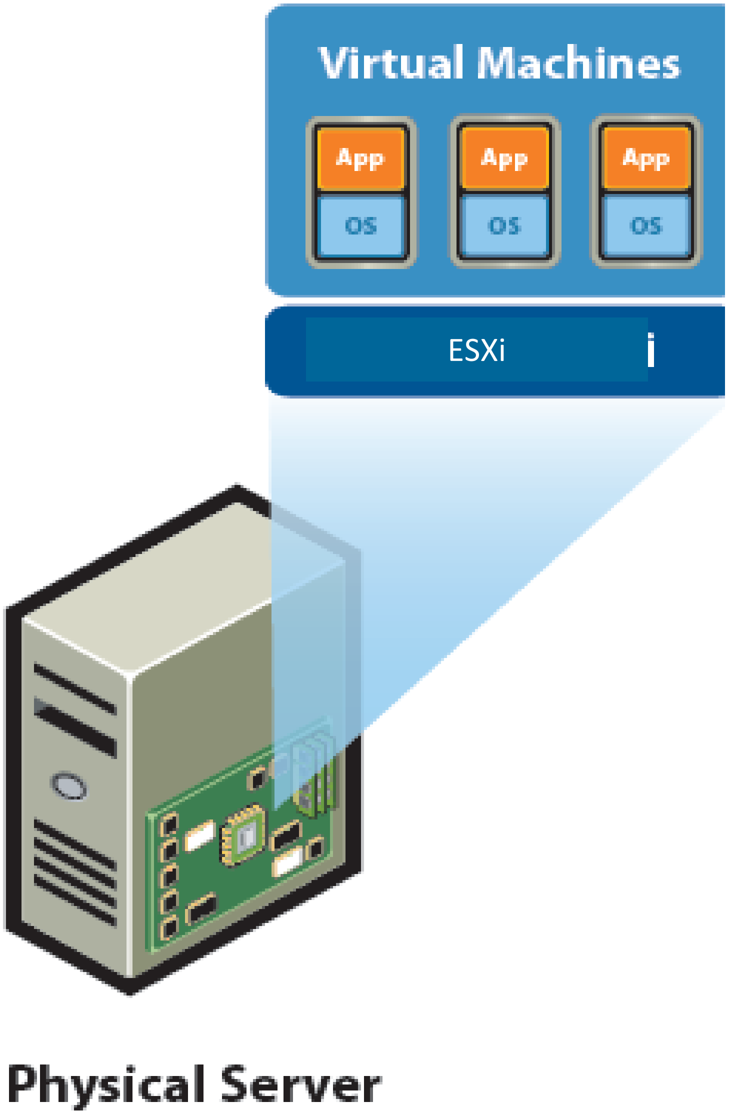
How do we secure our Virtual Infrastructure?

Use the Principles of Information Security

- Hardening and Lockdown
- Defense in Depth
- Authorization, Authentication, and Accounting
- Separation of Duties and Least Privileges
- Administrative Controls

The Future of Virtualization Security

VMware ESXi: The next step in Virtualization Security



Unmatched security and reliability:

- Compact 32MB footprint
- OS independence means minimal interfaces and a small attack profile
- Embedded in hardware --- reduces risk of tampering
- Unstructured Service Console management replaced by controlled API-based management
- Open ports highly limited.

Leveraging Virtualization To Solve Security Problems

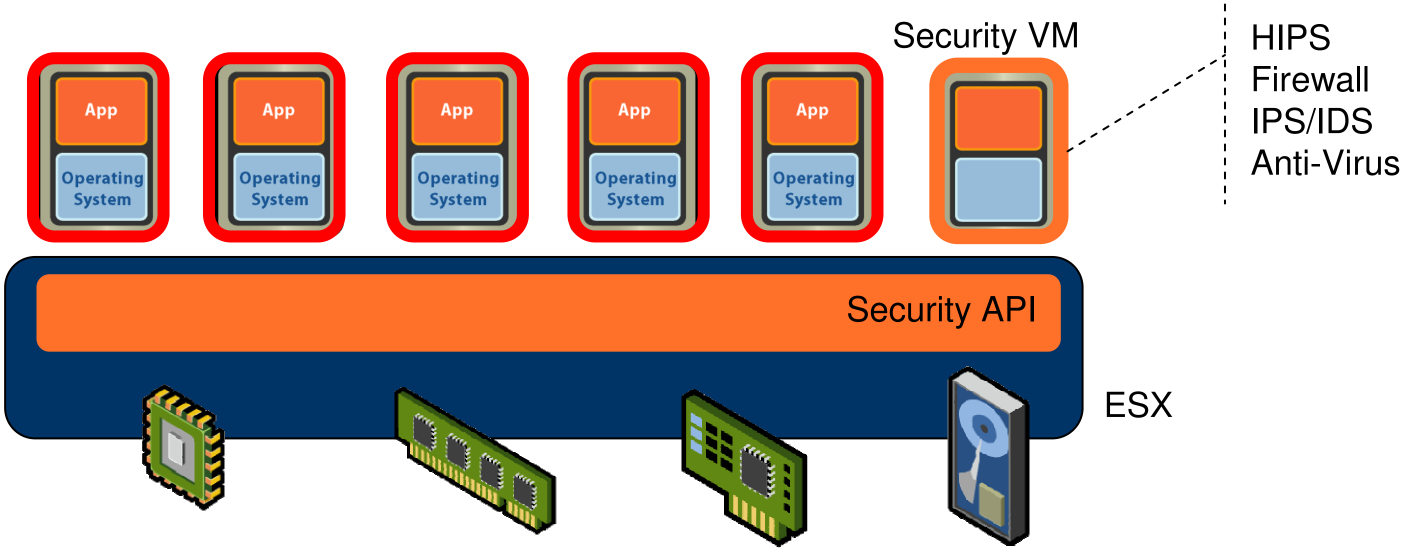
Security solutions are facing a growing problem

- Protection engines do not get complete visibility in and below the OS
- Protection engines are running in the same context as the malware they are protecting against
- Even those that are in a safe context, can’t see other contexts (e.g. network protection has no host visibility).

Virtualization can provide the needed visibility

- Better Context – Provide protection from outside the OS, from a trusted context
- New Capabilities – view all interactions and contexts
  - CPU
  - Memory
  - Network
  - Storage

Introducing VMsafe™



- New security solutions can be developed and integrated into VMware virtual infrastructure
- Protect the VM by inspection of virtual components (CPU, Memory, Network and Storage)
- Complete integration and awareness of VMotion, Storage VMotion, HA, etc.
- Provides an unprecedented level of security for the application and the data inside the VM

VMsafe™ APIs

API’s for all virtual hardware components of the VM

CPU/Memory Inspection

- Inspection of specific memory pages being used by the VM or it applications
- Knowledge of the CPU state
- Policy enforcement through resource allocation of CPU and memory pages

Networking

- View all IO traffic on the host
- Ability to intercept, view, modify and replicate IO traffic from any one VM or all VM’s on a single host.
- Capability to provide inline or passive protection

Storage

- Ability to mount and read virtual disks (VMDK)
- Inspect IO read/writes to the storage devices
- Transparent to the device and inline of the ESX Storage stack

Best Practices References

- Security Design of the VMware Infrastructure 3 Architecture (http://www.vmware.com/resources/techresources/727)
- VMware Infrastructure 3 Security Hardening (http://www.vmware.com/vmtn/resources/726)
- Managing VMware VirtualCenter Roles and Permissions (http://www.vmware.com/resources/techresources/826)
- DISA STIG and Checklist for VMware ESX (http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf) (http://iase.disa.mil/stigs/checklist/esx_server_checklist_v1r1_30_apr_2008.pdf)
- CIS (Center for Internet Security) Benchmark (http://www.cisecurity.org/bench_vm.html)
- Xtravirt Virtualization Security Risk Assessment (http://www.xtravirt.com/index.php?option=com_remository&Itemid=75&func=fileinfo&id=15)