

Securing the Virtual Environment

January 13, 2012

Nathaniel C. Gravel, CISA, CISM, CRISC
Director – Information Security Practice



GraVoc Associates, Inc.

- Founded in 1994
- Located in Peabody, MA
- Organized into 5 Practices
- Information Security Practice:
 - 1) Risk Management & Compliance
 - 2) IT Assurance
 - 3) Audit



Today's Agenda

- Introduction
- Key Components & Challenges
- Applying Existing Security Strategies
- Challenges and Control Considerations by Component
- Top Five Areas of Impact
- Question & Answer
- Conclusion



Introduction: Presentation Objectives

- 1) Develop an understanding of the security challenges posed by virtualization.
- 2) Provide control considerations and recommendations for securing the virtual environment.
- 3) Provide criteria for future risk assessment and risk management activities.

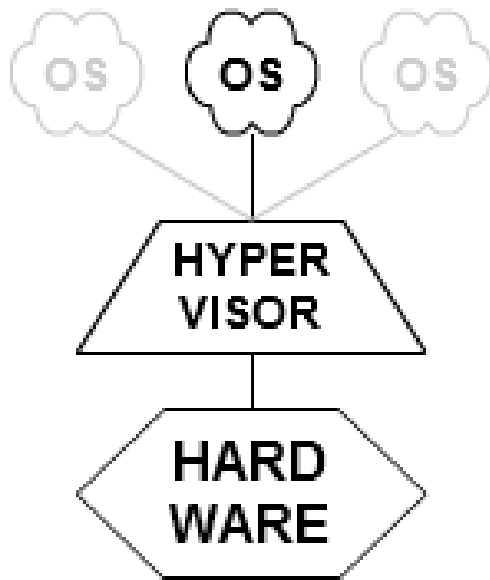


Introduction: Disclaimers & Definitions

- Today's Discussion:
 - 1) Non-Platform Specific
 - 2) Full Virtualization
 - 3) Server Virtualization
- Hypervisor – Control Panel
- Host OS – Pertains to Hypervisor
- Guest OS – Pertains to Virtual Machine

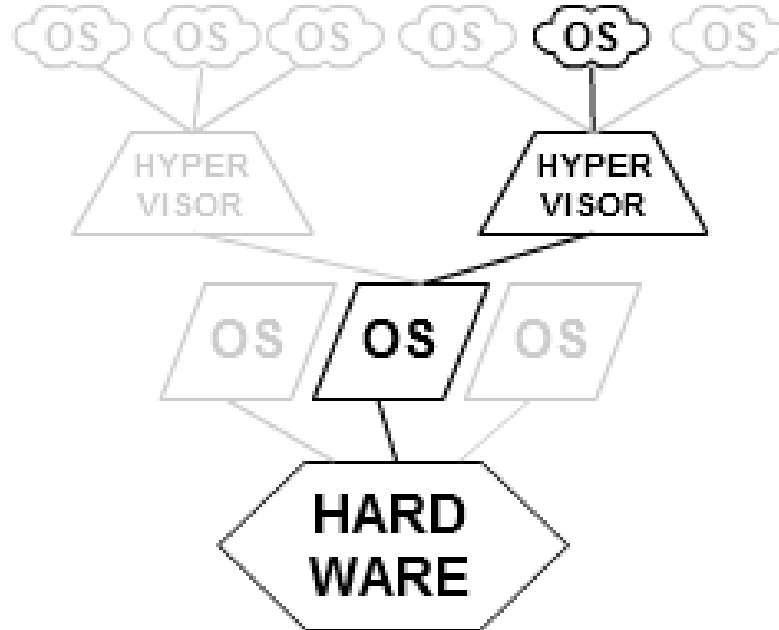


Full Virtualization Architectures



TYPE 1

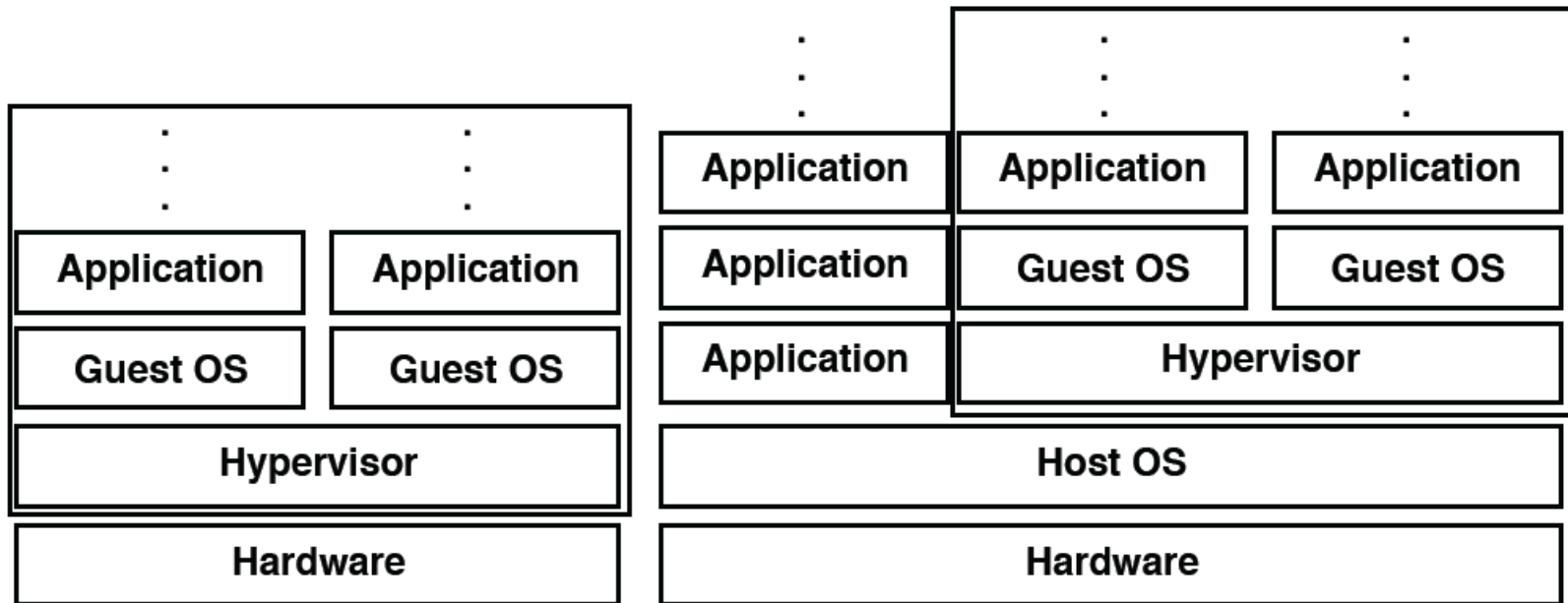
*native
(bare metal)*



TYPE 2

hosted

Full Virtualization Architectures



Bare metal

Hosted

Securing the Virtual Environment: Key Components

- Hypervisor
- Host System & Host OS (Type 2)
- Guest OSs (Virtualized Hardware)
- Installed Applications
- Virtualized Storage
- Virtualized Networking



Securing the Virtual Environment: Three Principal Challenges

Complexity of Administration

- Learning Curve for IT Staff
- Another Network to Manage
- Connecting Physical and Virtual Assets



Securing the Virtual Environment: Three Principal Challenges

Lack of Visibility

- Limitations of Audit and Monitoring Capabilities
- Rogue VMs
- Configuration Management



Securing the Virtual Environment: Three Principal Challenges

Non-Compliance with Established Policy/ `Procedure

- Network Administration, Auditing, and Monitoring
- SDLC and Change Management
- Patch Management, Anti-virus, Anti-spyware, Malware



Applying Existing Security Strategies

- Physical Security
- Policies & Procedures
- System Hardening
- Access Controls
- Data Loss Prevention
- System Auditing & Monitoring
- Configuration & Resource Management



Challenge: Hypervisor Security

- Single Point of Failure
- Increased Impact of Loss/Compromise
- Local and Remote Administration
- Networking & Communications
- Patch Management
- Data Storage



Hypervisor Control Considerations

- Restrict physical access to host system
- Disconnect unused physical hardware and NICs from host system
- Install all necessary patches to hypervisor and host OS (if applicable)



Hypervisor Control Considerations

- Restrict administrative access and establish administrative access levels
- Establish a dedicated management network or encrypt management network communications
- Disable unnecessary services such as clipboard and file sharing



Hypervisor Control Considerations

- Enable introspection capabilities to monitor security of each guest OS
- Enable introspection capabilities to monitor security of activity occurring between guest OSs
- Monitor hypervisor itself and enable self-integrity monitoring capabilities.



Hypervisor Control Considerations

Type 2 (Host OS)

- For host OS, minimize the number of applications installed other than hypervisor
- For host OS, take measures to secure and ensure integrity of other applications



Challenge: Guest OS Security

- Sharing (Guest Tools)
- Side-Channel Attacks
- Escape
- Time Synchronization
- Software Licensing
- Access to Storage
- System Development Lifecycle (SDLC)



Guest OS Control Considerations

- Group guests of similar risk-level on the same hypervisor or host
- Isolate each guest OS through physical and/or logical partitioning (sandboxing)
- Enable introspection capabilities to facilitate guest OS monitoring.



Challenge: Images & Snapshots

- Duplication of Sensitive Data
- Accessibility and Portability
- Patching and Configuration Changes
- Tracking
- Proliferation of Images (Sprawl)



Control Considerations for Images & Snapshots

- Configure permissions to limit the number of administrators and end-users who can create images (no access, read-only, write)
- Implement formal image and snapshot management policies and procedures that govern image creation, security, distribution, storage, use, retirement, and destruction
- Restrict guest OS access to virtual hardware



Challenge: Virtual Networking

- Schema and Design
- Switching and Balancing Traffic
- Integration with Physical (Wired) Network
- Consistency with Established Protocols



Virtual Network Control Considerations

- Consider establishing a virtual LAN (VLAN) and investigate VLAN monitoring tools.
- Consider the use of APIs on the hypervisor
- Consider establishing a separate set of network management or monitoring policies for the virtual network



Virtualization: Top Five Areas of Impact

1) Policies & Procedures

- Network Administration, Auditing, and Monitoring
- Patch Management, Anti-virus, Anti-spyware, Malware
- SDLC and Change Management
- Disaster Recovery/Business Continuity Plan

2) IT Asset Inventory & Network Diagrams

3) Risk Assessment and IT Assurance Testing

4) Vendor Contracts and SLAs

5) Budget & IT Strategic Planning



Question & Answer



Suggested Reading

- NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies
- ISACA Whitepaper (October 2010): Virtualization: Benefits and Challenges
- Platform-Specific User Manuals & Security Guides



Thank You!

Nathaniel C. Gravel

Director – Information Security Practice

GraVoc Associates, Inc.

nateg@gravoc.com

978-538-9055 ext. 129

