Foundstone
A division of McAfee

Putting Security in Perspective for Virtualization

Shanit Gupta

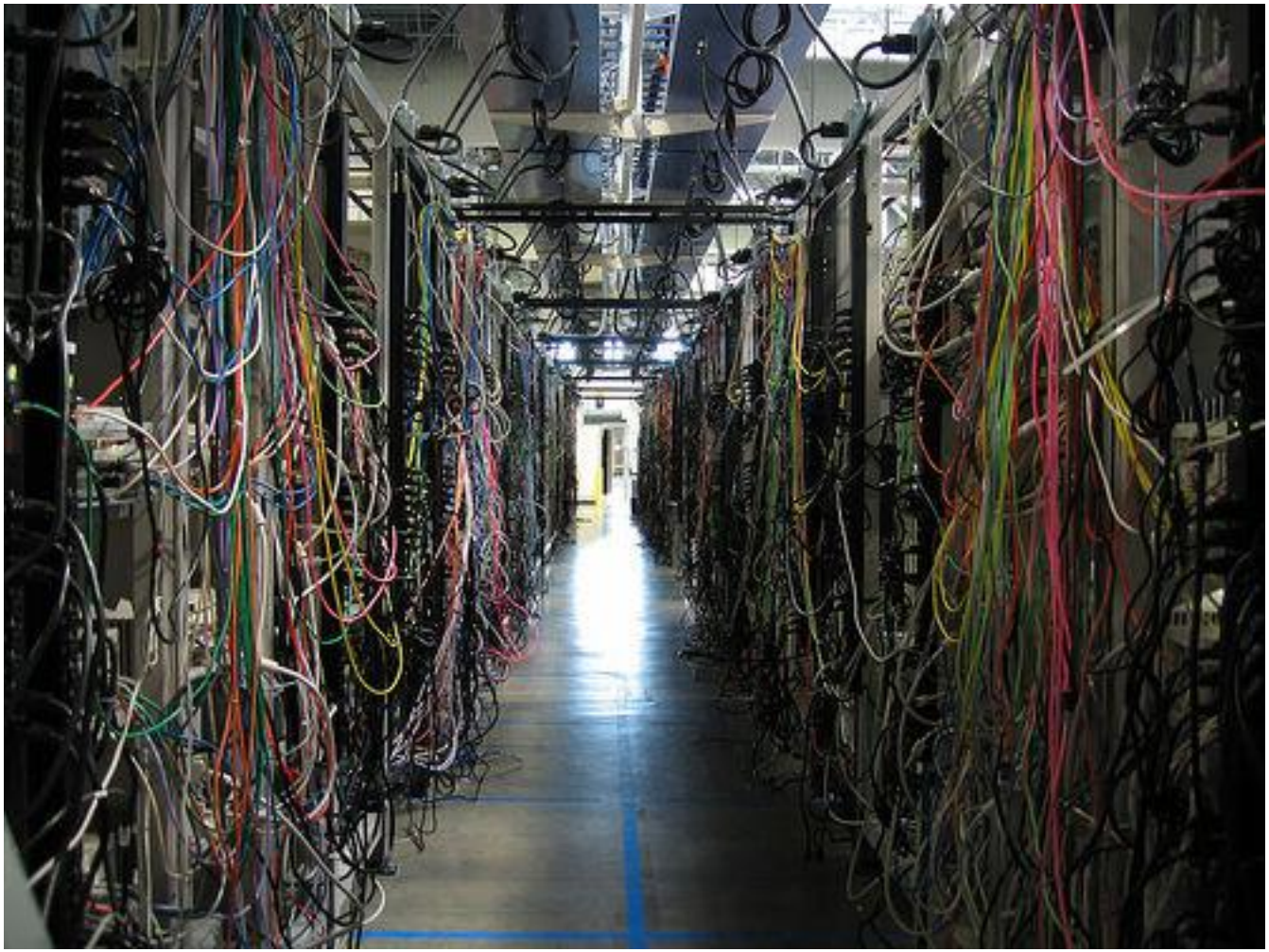
Principal Consultant,
Foundstone Professional Services

February 6th, 2009

Today's Agenda

- Introduction
- Virtualization Myths
- Virtualization Technology
- Security in a Virtualized World
  - Goals
  - Risks
- Is the picture bleak?
- Building Security from the Start
  - People
  - Process
  - Technology
- Parting Thoughts

Why Virtualize?



Virtualization – More Than a Fad

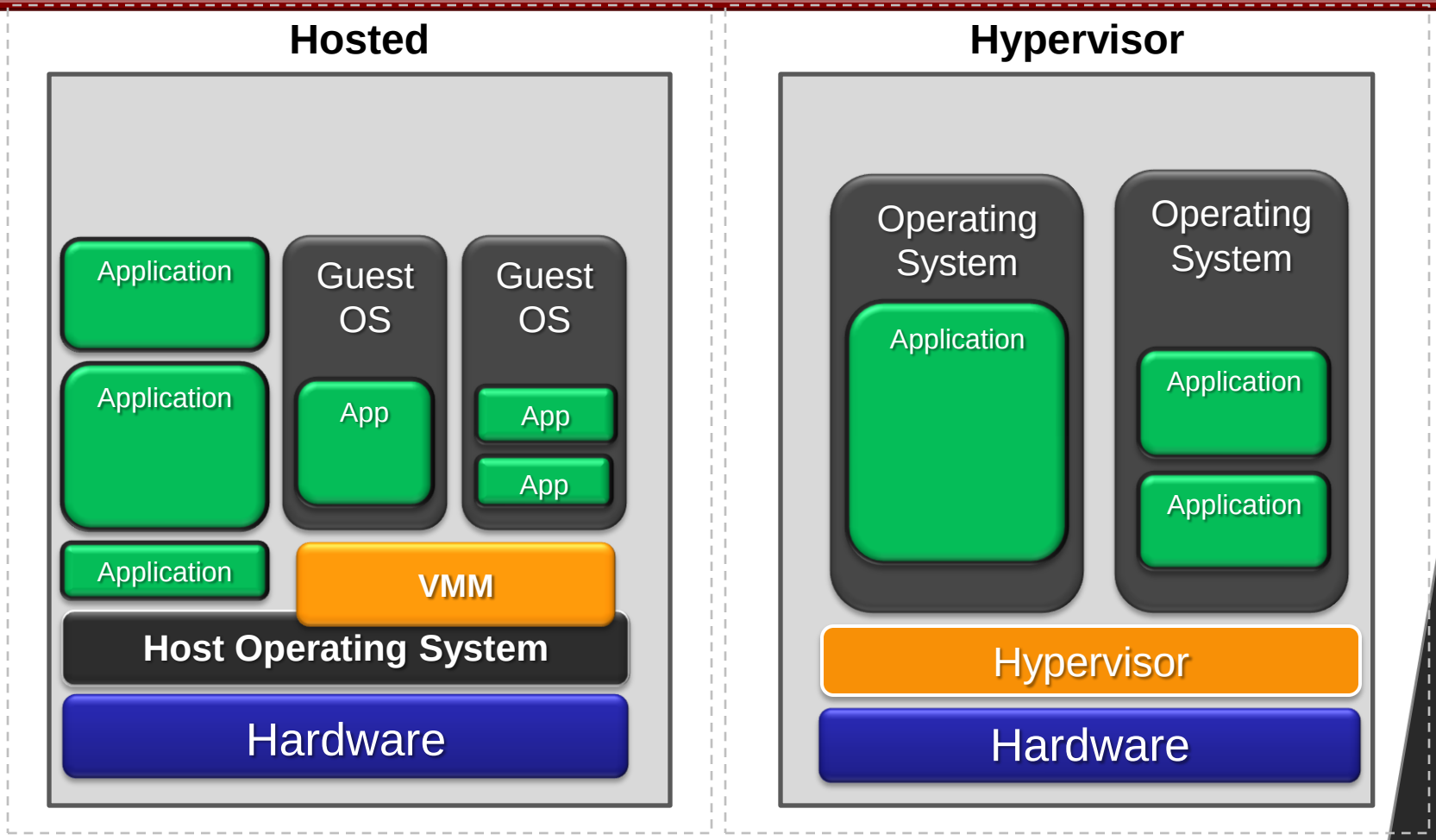
According to Gartner, virtualization is one of the hottest topics in IT…

Yet…only one in eight enterprises have a formal security or information protection strategy for their virtual infrastructure (according to InfoWeek)

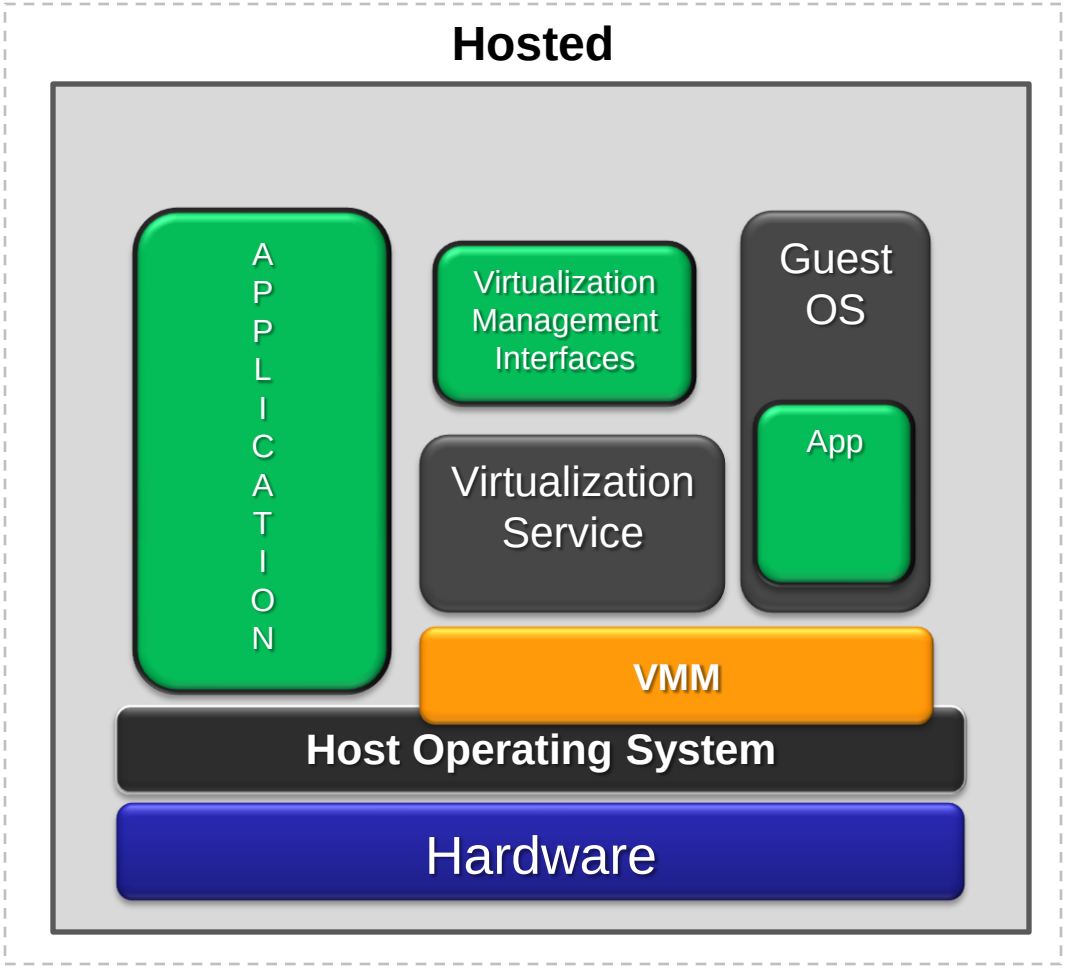
MYTHBUSTERS

- Only the Host needs to be patched
- The Host protects the VMs
- VMs are more/less secure
- Virtual Isolation can be bypassed by default
- There is no downtime in virtualized environment
- Administrator on Host can NOT compromise the VM

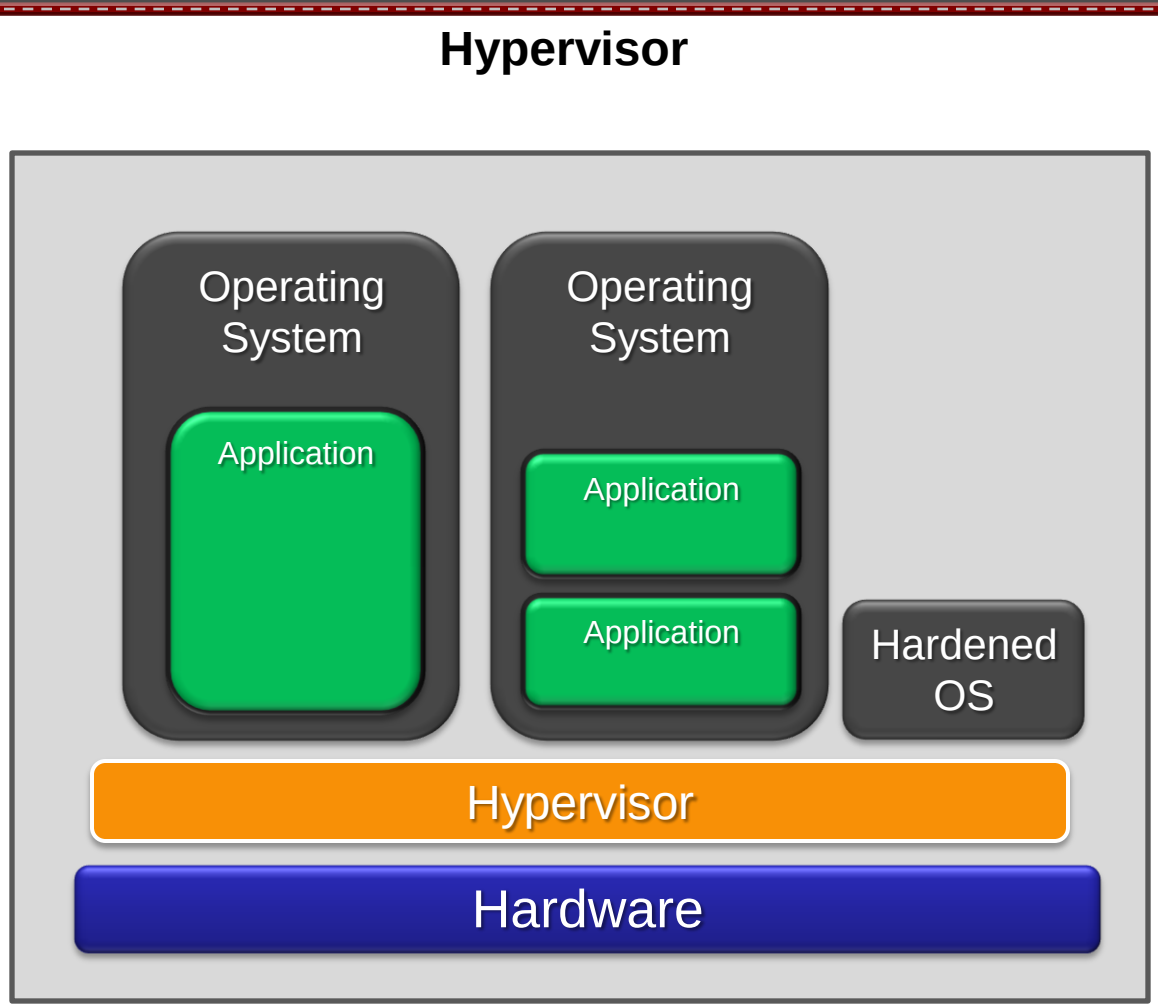
Virtualization Techniques



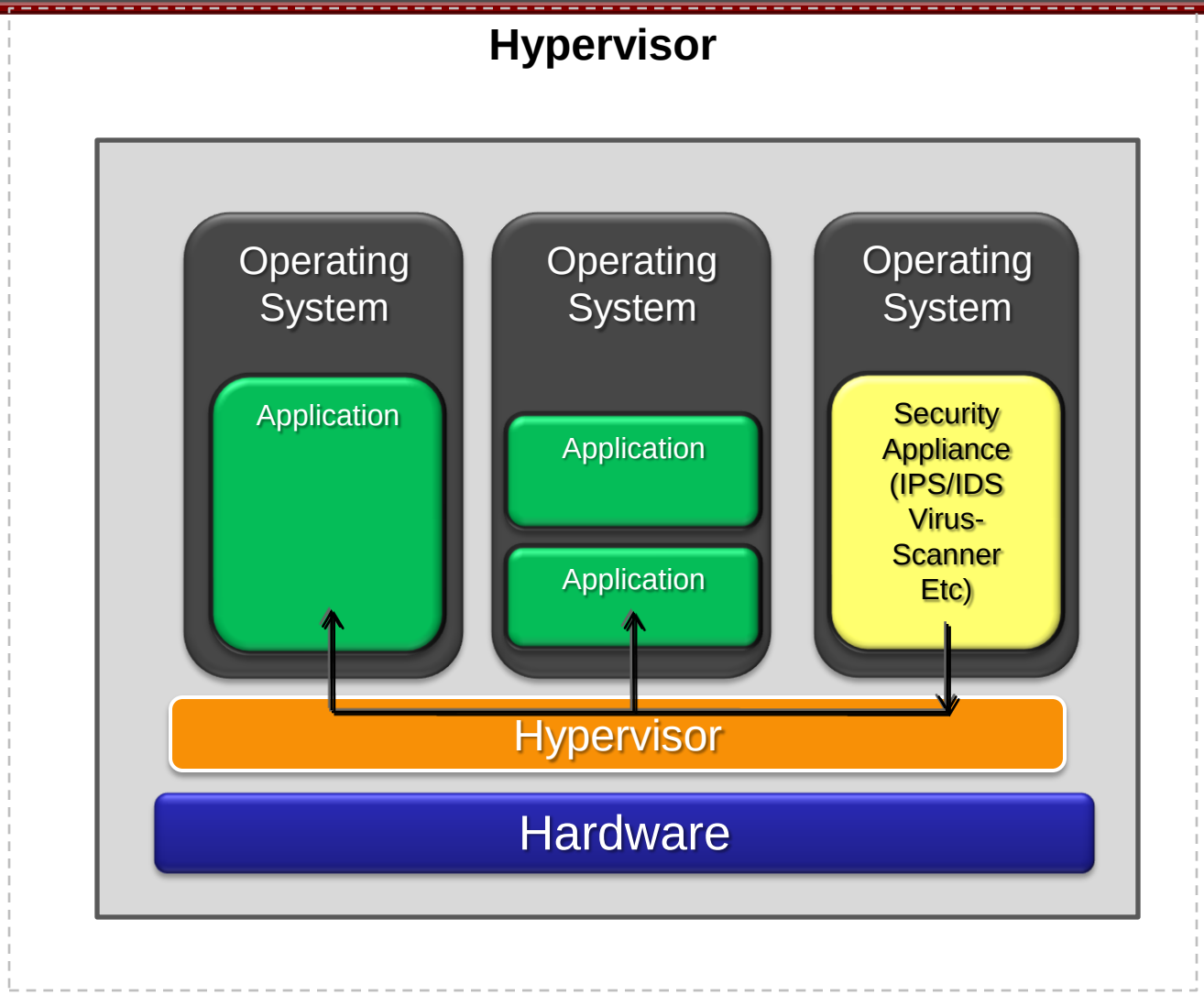
Hosted Architecture



Hypervisor


Hypervisor
Operating System
Application
Operating System
Application
Application
Hardened OS
Hypervisor
Hardware

Virtual Appliances



Virtualization Attacks

- **SubVirt – *Samuel T. King, Peter M. Chen: Michigan U***

  Kernel based Rootkit based on a commercial VMM, which creates and emulates virtual hardware.

- **BluePill – *Joanna Rutkowska***

  Moves the Host OS to a Virtual Machine

- **Vitriol – *Dino Dai Zovi***

  VM Rootkit targeting Mac OSX

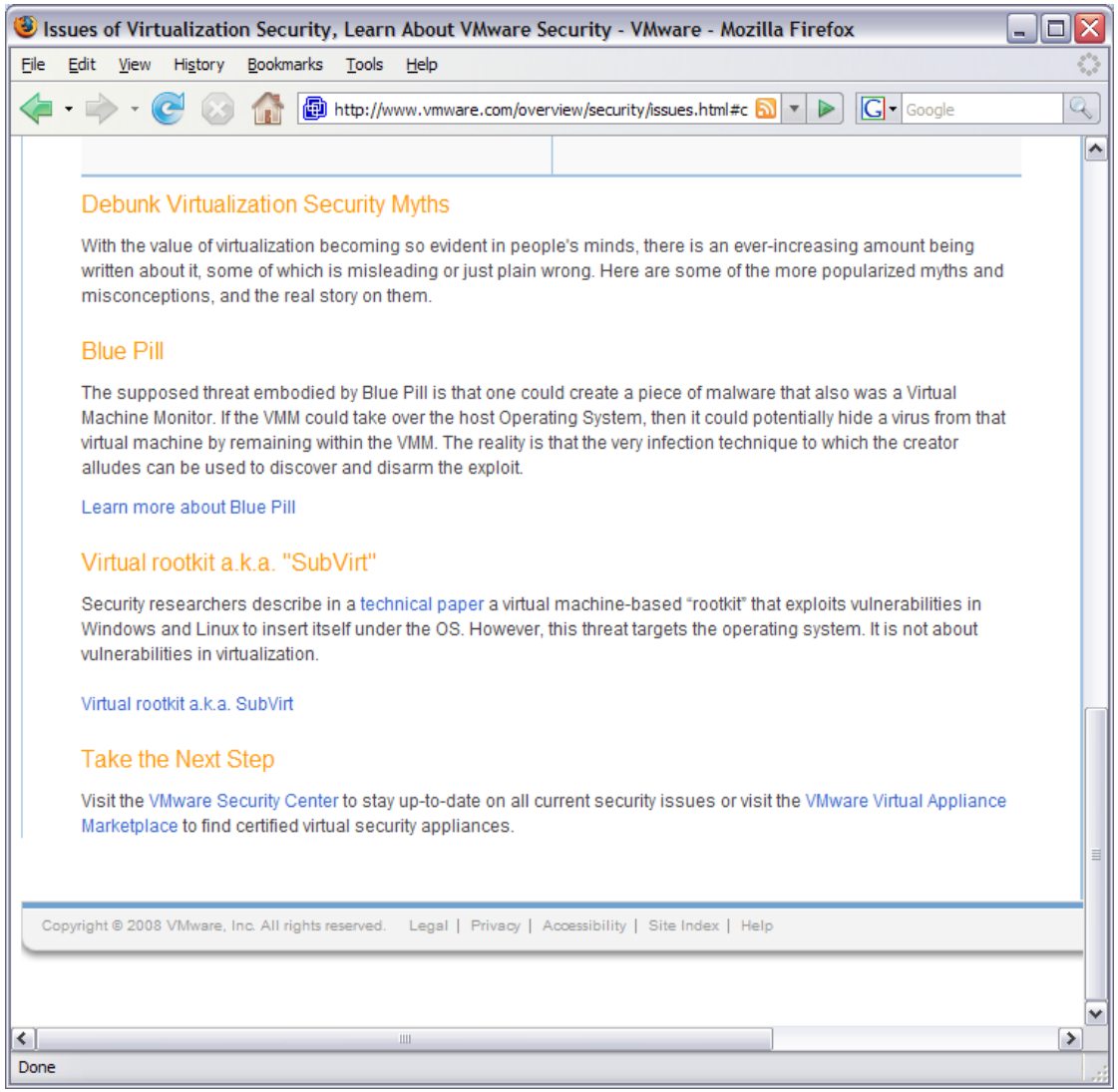
- **Detecting a Virtual Environment**

  RedPill / NoPill / scoopy_doo

- **Xensploit – VMotion tampering**

  University of Michigan

Virtualization Myths

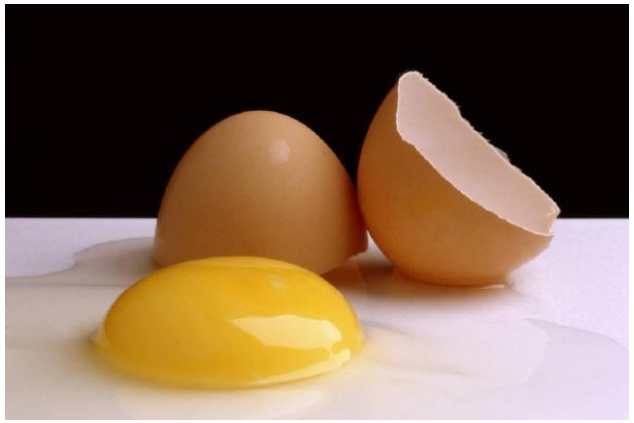


Security Goals

- Guest Isolation
- Resource Protection
- Data Communication
- Authorization Controls
- Emulate Physical World

Risks to Virtualization

- Shell Breakage
  - Guest to Host
  - Guest to Guest
  - Guest to .*
- Asset Tracking and Management
- Viruses / Worms
- Public Disclosures
- Configuration Gotchas
- Maintenance Nightmares



The Expanded Attack Surface

- Host OS
- Virtual Machine OS
- VM Hard Disk Storage
- VM Configuration Files
- Remote Management Interfaces
- Network Segments
- Asset Management
- Virtual Appliances

Host OS

- Harden the Host
  - MAC Settings
  - IP Filters
  - Promiscuous Mode
  - Shared Memory
  - Shared Folders
  - Drag and Drop
- Patch Regularly
- Control User Permissions

Virtual Machine OS

- Just like a Physical Server
  - Patch
  - Harden
  - Secure – Anti-Virus, Backup, Firewall …
  - User Accounts

Virtualization Data Storage

- Access to VM files
  - File System for VM
  - Configuration Settings
- Network Storage Devices
  - Network based ACLs
  - Authentication on NAS/SAN
  - Authorization on NAS/SAN
  - Masking, Zoning

Remote Management Interface

- Tools used for Remote Management
  - Not all are equally secure
- Access to Tools and Management System
- User Permissions
- Auditing and Logging of User Operations
- Network Segmentation for Management
- Configuration of Management Tools
  - SSL
  - RDP

Network Segmentation

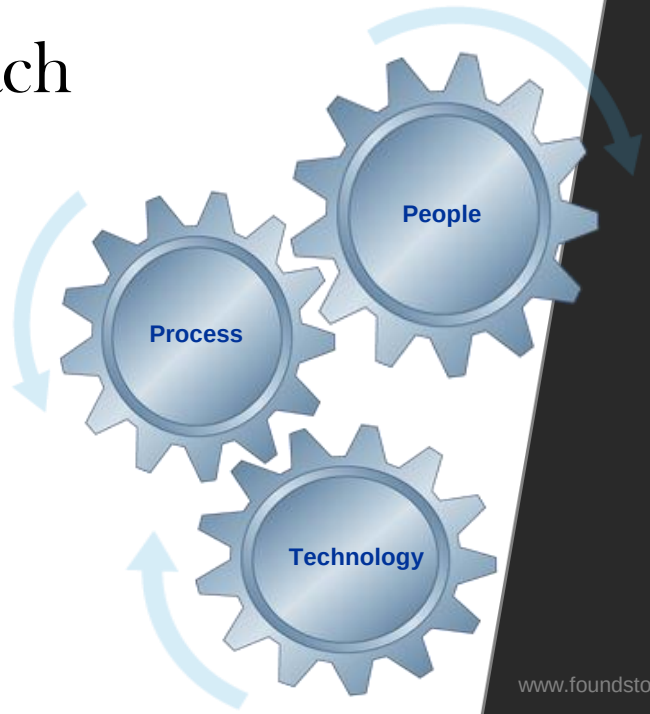
- Segment the Network
- Design VLANs
  - Management
  - Storage
  - Development / Test
  - Production
- IPSec
- Network Access Controls
  - IDS/IPS
  - Firewalls

Virtual Appliances

- Watch out for VM based Solutions
- Will hold keys to the Kingdom
- Many will be Snake Oil – Beware!

Building in Security from the Start

- Important to fully assess your environment and plan virtualization and security together
- Approach needs to move from reactive to one of strategic planning and execution
- Classic risk management approach is best, focusing on:
  - People
  - Processes
  - Technology



People

- What is the level of expertise?
- Are they expected to be security experts?
- Information is available for FREE

Management Support

- Directives are NOT enough
- Need Dedicated Resources
- Need to Invest In Training
- Planning and Execution Requires Time

Process

- Risk Assessment & Treatment
- Asset Management
- Communication and Operations Management
  - System Hardening
  - Network Architecture Design
  - Performance Monitoring & Capacity Planning
  - Backup
  - Logging and Auditing
- Incident Management / Response
- Compliance
  - SOX
  - PCI

Compliance

- SOX
  - Standardize server configuration
- PCI
  - Firewalls
  - Anti-Virus
  - Patching
  - Restrict access
  - Logging and Auditing

Technology

Technology..

- Anti-Virus
- Host based IDS / IPS
- File integrity checkers
  - Tripwire for ESX Server
- Virtual Appliances

Final Thoughts …

"The most dangerous risks are the ones that are never considered, or considered too late. Executives need to look to the future. IT risk management is working the way it should when it is simply part of the way the company does business."

- Richard Hunter
group vice president and Gartner fellow

More Information on Virtualization

- www.foundstone.com/virtualization
- Compliance - http://www.vmware.com/technology/security/compliance/resources.html
- Download our Risk and Virtualization white paper at www.foundstone.com/wp
- Questions? consulting@foundstone.com

Thank you!