Education

Unmasking Virtualization Security

Eric A. Hibbard, CISSP, CISA
Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Unmasking Virtualization Security

As enterprises adopt virtualization technologies in their data centers, it is important to understand the risks and to employ protective measures appropriate to the sensitivity and criticality of the data. Special attention is required for storage-based technologies to ensure both data security and data resilience. In addition, cloud computing has a heavy reliance on virtualization, which can be a source of problems if not handled correctly.

This session summarizes the key threats and their relevance, outlines strategies for addressing the risks, and describes the relevant virtualization security technologies that should be considered.

Virtualization Overview

Background

- Storage virtualization plays an important role in data resilience and data protection strategies within many organizations.
- Migrations onto virtual servers have saved some businesses huge sums of money as a result of consolidation and improved efficiency.
- The server virtualization market has emerged so quickly that customers have not been able to keep up from a best practices standpoint (especially security).
- Server virtualization introduces technologies that must be managed and secured.
- Virtualization is clearly an enabler for cloud.

Virtualization Issues

- Networks that work correctly with physical servers don't necessarily work well with virtual machines.
- Virtualization introduces technologies – like the hypervisor – that must be managed.
- Virtual switching, which routes network traffic between virtual servers, is often done in ways that aren't always visible to tools designed to monitor traffic on the physical network.
- Many business continuity failures in virtualized environments can be attributed to network design flaws.
- In many organizations, the IT security team isn't consulted about virtual infrastructure until well after the architecture is built and rolled out on production servers.
- Virtualization does present risks if best practices are not followed and adapted to a virtual infrastructure.
- Virtual server instances may move between data centers, not just within a single facility.

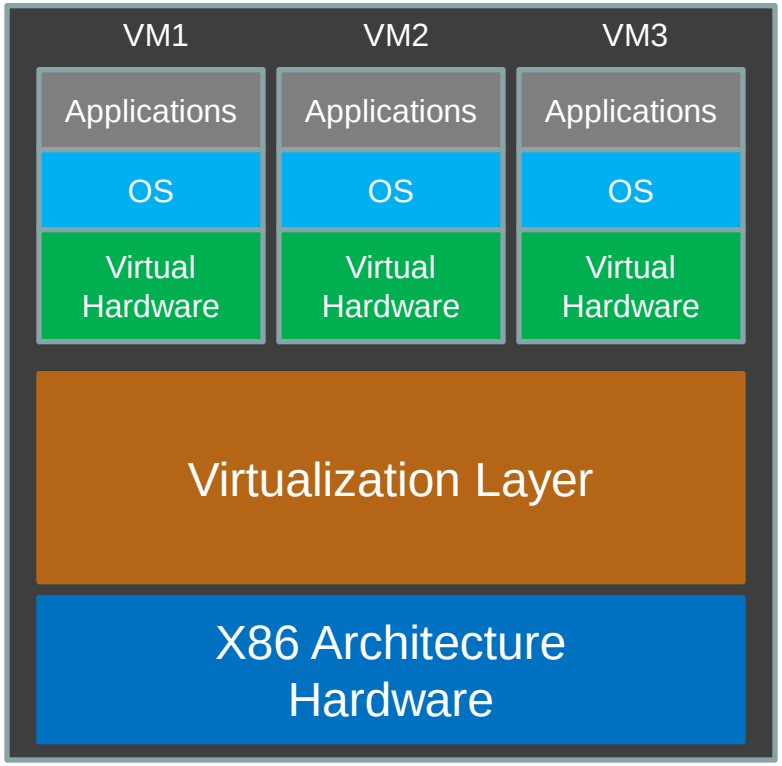
Key Virtualization Components

- **Virtual Machine (VM):** Software that allow the sharing of the underlying physical machine resources between different VMs, each running its own operating system.
- **Virtual Machine Monitor (VMM):** Software responsible for managing interactions between VM(s) and the physical system.
- **Hypervisor:** The software that handles kernel operations. A hypervisor can run on bare hardware (Type 1 or native VM) or on top of an operating system (Type 2 or hosted VM).
- **Virtual Networks:** Virtual networks tie together the VMs' virtual network interface cards (*vnics*), virtual switches (*vswitches*), and physical network interface cards (NICs) into various network architectures.
- **Putting It All Together:** A virtualized environment consists of a VMM and one or more VMs. The VMs and VMM interact with either a hypervisor or a host OS to access hardware, local I/O, and networking resources. In addition to these components, virtualization architectures leverage virtual networking, virtual storage, and terminal service capabilities to complete their architectures.

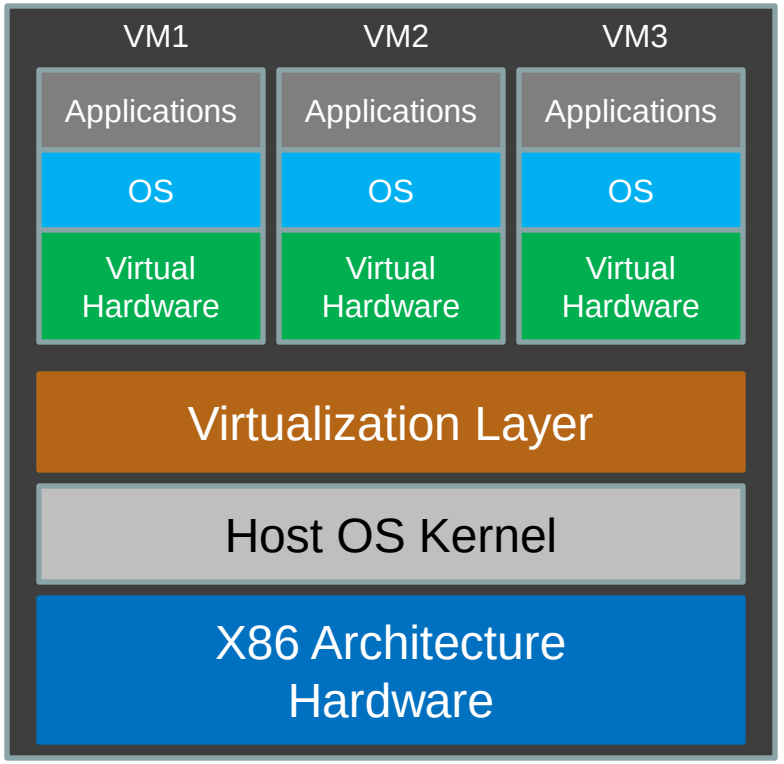
Key Virtualization Types

Education SNIA

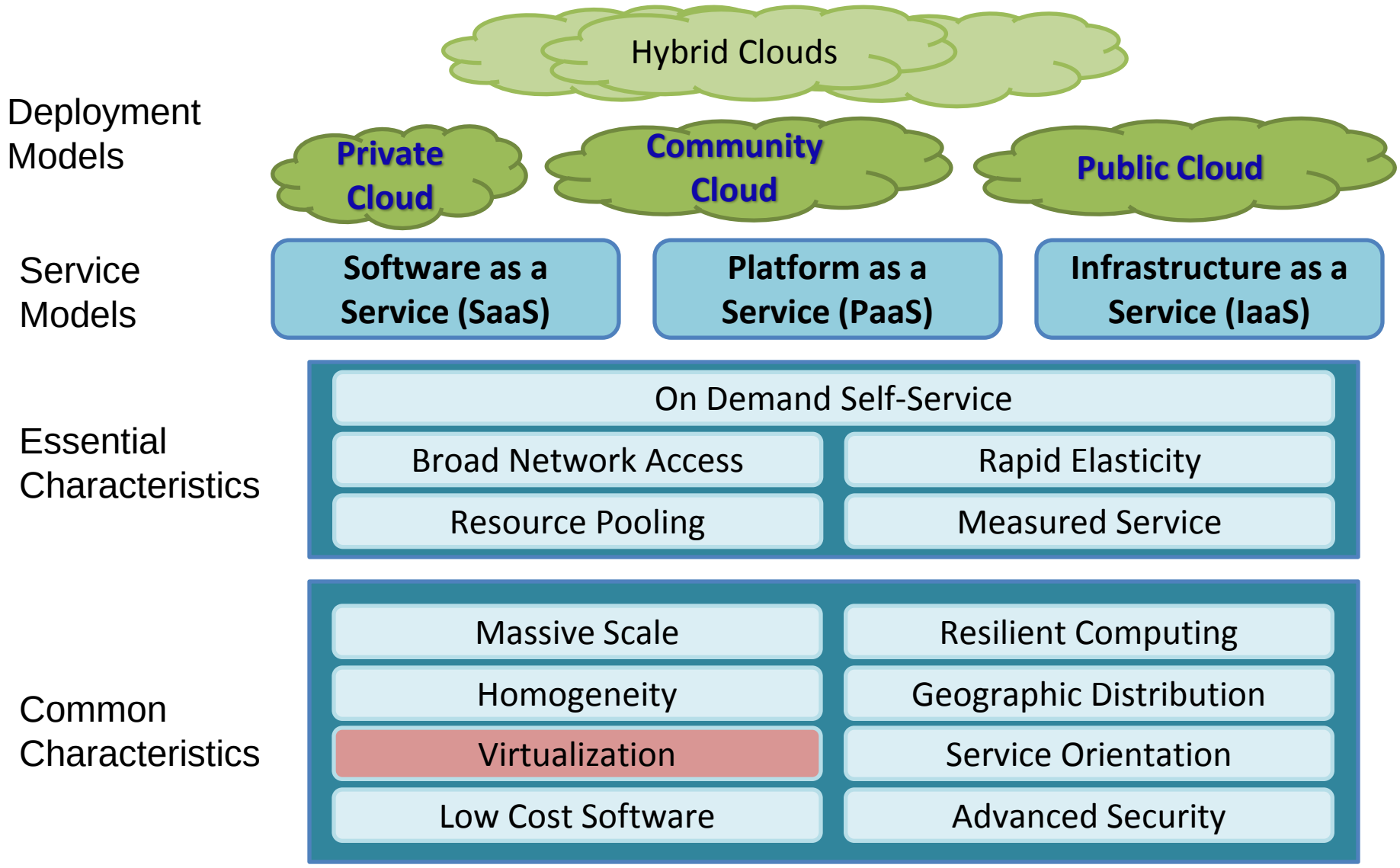
Type 1 Virtualization (Bare Metal)



Type 2 Virtualization (Hosted)



NIST Cloud Definition Framework



Storage and Virtualization

- Storage virtualization is employed by many organizations as part of the data resilience and disaster recovery and business continuity solutions
- An assortment of storage security mechanisms exist:
  - Entity authentication (iSCSI CHAP & FC-SP DH-CHAP)
  - Source filtering (IP address & WWNs)
  - At-rest encryption (HBA and in-line)
- Storage security mechanisms often have to be loosened to accommodate server virtualization
- Storage-based replication can be a powerful compliment for VM movement between sites

The Attack Surface

Virtualized Threat Vectors
(Beyond the Usual Suspects)

- Host/Server
  - Management interfaces
  - Virtual OS controls
  - Hypervisors
  - Multi-tenancy
- Network
  - Virtualized networking
  - Malware (Worms)
- Storage
  - Virtual disks

Hyper-escalation vulnerabilities

- Guest VM "breaks out" (i.e., escapes its isolation and maliciously interacts with the hypervisor)
- Guest VM escalates privileges with regard to other Guests
- Guest VM escalates privileges with regard to Host
  - Could go so far as to fully compromise Host

- Unprivileged user escalation
  - Denial of Service vulnerability allowing an unprivileged user to crash the system
  - Vulnerability allowing an unprivileged user to escalate privileges within the guest VM

Virtualization Security

Observations & Trends

- Concerns over security in a virtual environment are often centered around lack of visibility, lack of control and fear of the unknown.
- Smaller organizations with minimal IT departments can see improved security when using services and infrastructure from a public cloud service provider.
- The security and IS audit communities continue to highlight the risks associated with the use of cloud
- The storage industry is becoming very excited about virtualization and enabling technologies for the cloud
- In the U.S., many lawyers have become very ***interested*** in the cloud (data breaches and lawsuits)

Immutable Laws of Virtualization Security

- ***Law 1:*** *All existing OS-level attacks work in the exact same way.*
- ***Law 2:*** *The hypervisor attack surface is additive to a system's risk profile.*
- ***Law 3:*** *Separating functionality and/or content into VMs will reduce risk.*
- ***Law 4:*** *Aggregating functions and resources onto a physical platform will increase risk.*
- ***Law 5:*** *A system containing a "trusted" VM on an "untrusted" host has a higher risk level than a system containing a "trusted" host with an "untrusted" VM.*

SOURCE: Burton Group, *Attacking and Defending Virtual Environments*, Version 1, Pete Lindstrom, Jan-2008, http://www.burtongroup.com/Download/Media/AttackingAnd.pdf

Virtualization Security Issues

- Virtualization potentially makes the strong perimeter defense obsolete.
- While technologies are available to secure virtual infrastructure, it is common to see security failures that can be tracked to misconfigurations.
- The traffic flowing between VMs is another area of concern, since IDS/IPS, firewalls and other monitoring tools aren't able to tell if those machines are running on the same physical server hardware.
- In the virtual world, there is no inherent separation of duties, so it has to be build in.
- In an unchecked, unmonitored virtual environment, administrators are all powerful; often they don't understand the security risks.
- The hypervisor must be patched just like any other operating system to plug security holes.

Virtualization Security Guidance

Best Practices for Virtualized Systems

- Harden the Host Operating System, Hypervisor, and VMs
- Limit Physical Access to the Host
- Use Encrypted Communications
- Disable Background Tasks
- Employ Timely Patching and Updating of Systems
- Enable Perimeter Defenses on the VM
- Implement Only One Primary Function per VM
- Implement File Integrity Checks
- Perform Image Backups Frequently
- Secure VM Remote Access

SOURCE:
***Cloud Security*, Krutz, Vines, 2010, Wiley Publishing, ISBN: 978-0-470-58987-8.**

Virtualization Questions to Ponder
(Before moving to fully virtualized environments)

- How will our current analysis, debugging, and forensics tools adapt themselves to virtualization?
- What new tools will security administrators be required to master between all of the virtualization platforms?
- How does patch management impact the virtual infrastructure for guests, hosts, and management subsystems?
- Will new security tools, such as hardware virtualization built into CPUs, help protect the hypervisor by moving it out of software?
- How will known security best practices, such as no-exec stacks, make a difference when fully virtualized? Will hardware virtualization pave the way to a truly secure VMM?
- For shared storage, what changes to the storage security controls (e.g., encryption, FC-SP, etc.) are necessary? If the storage security controls need to be relaxed, what are the implications?

Final Thoughts

Summary

- The benefits of virtualization are obvious: *more bang for your buck* (i.e., doing more with less).
- Server virtualization is common-place for many organizations, and becoming so for many others
- The concept that virtual operating environments are just as secure as their physical counterparts can be a very expensive and destructive fallacy
- Virtualization security is a viable option, but:
  - Security professionals need to be engaged early
  - Security requirements/mechanisms may impose restrictions that negate some or all of the value of virtualization
  - Compliance requirements must be factored into the solution
- Storage technologies can be leveraged to help with data management

Conclusions

- Security of virtual machines and environments is typically not considered, not because the security of these implementations is a technological mystery, but because it is generally an unknown vector by the groups that are implementing wide-spread virtualization.
- Virtualization should not be taken for granted in the security realm, and should instead be treated as more of a daily threat than physical and single-purpose operating systems and appliances.

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Attribution & Feedback

The SNIA Education Committee would like to thank the following individuals for their contributions to this Tutorial.

Authorship History

Eric A. Hibbard – September 2012

Updates:
N/A

Additional Contributors

SNIA Security TWG

Walter Hubis
Alan Yoder

Please send any questions or comments regarding this SNIA Tutorial to
tracktutorials@snia.org