

Virtualization, Security and Compliance

Mario D. Santana

Director, Secure Information Services

B E Y O N D A V A I L A B I L I T Y

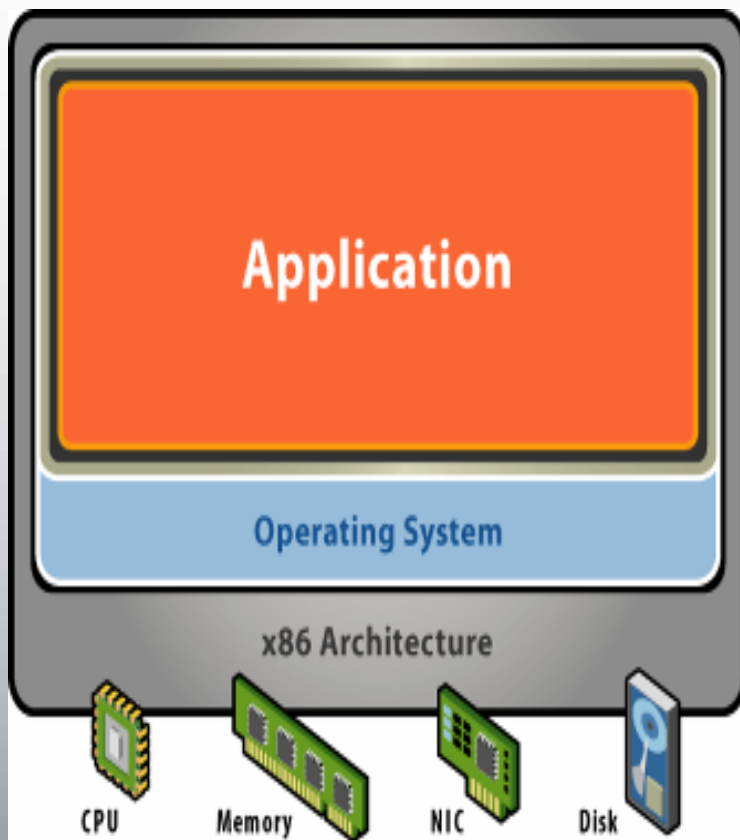


Agenda

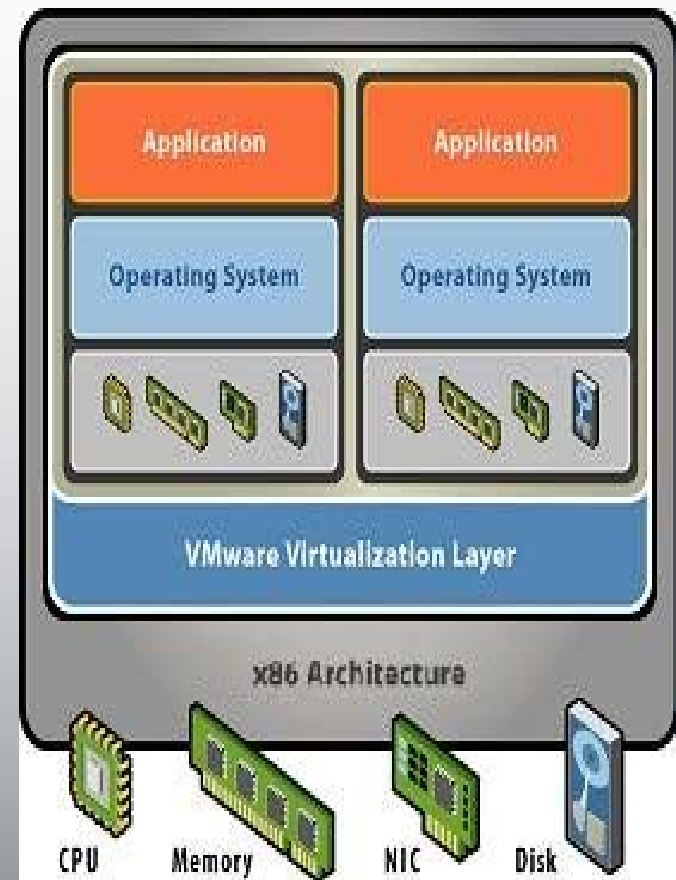
- **What v12n is and isn't**
- Virtual security hype
- Truly new issues
- Compliance impact
- Conclusion

V12N is hardware virtualization

Before Virtualization



After Virtualization



V12N is pretty cool!

- Run multiple VMs on a single PM
 - You can also spread VMs around multiple PMs
- Each VM looks like a PM to the OS/SW on it
 - This is because it kind of is. Sort of.
- A VM “is” a bunch of files in a directory
 - Copy/move/rename/delete – File operations on machines
 - Think of the file as a “live hibernation” file: keeps state
 - You still need the hypervisor, of course...
- A VM “is” the hypervisor and related management software
 - Add hardware or network connections to the VM with a click
 - You still need the files to store disk and memory data, of course...

V12N is not magic!

- Let's be clear: There's nothing we can do in a virtualized platform that we can't do in a (flexible) physical platform.
 - Theoretically, anyway. We'll come back to this...
- VMs expose hardware to the OS/SW on it in much the same ways as PMs
- Security issues are very similar
 - Missing patches still leave you vulnerable
 - Unnecessary services are still a risk
 - Weak passwords make just as ripe a target
- Think of a VM as a real machine. It kind of is. Sort of.
 - A real machine with software-as-hardware

Agenda

- What v12n is and isn't
- **Virtual security hype**
- Truly new issues
- Compliance impact
- Conclusion

Virtual IDS is different! Really!

- They run on VMs, attach to virtual switches, and etc.
- They may monitor virtual switches, assessing traffic that never hits the physical wire
- Simple confusions are used as FUD
 - Virtual switching is configured differently than Cisco
 - Promiscuous mode can be tricky
- Today, IDS/IPS/AV/etc use the same principles, whether virtual or physical
 - This is changing, but we'll get to that later.
- Oh, wait. Virtual IDS isn't different. Really.

Worse Than Useless

- “Analyst Chris Wolf of Midvale, Utah-based Burton Group said that from a reliability standpoint, running applications on a VM may be even more secure than running them on a dedicated physical machine.”
 - Bridget Botelho, 9/24/07, ServerVirtualization.com
- This statement, and many, many more like it, are the scariest thing in virtual security
 - Unwarranted confidence is the #1 cause of security breaches.
- There is no more or less security *per se* in virtualized vs. physical machines

Agenda

- What v12n is and isn't
- Virtual security hype
- **Truly new issues**
- Compliance impact
- Conclusion

Truly new issues

- V12n's security relevance is with the v12n layer
 - Now, instead of attacking the hardware with hardware, you can attack the hardware with software – because *the hardware is software*.
 - Hypervisor as vulnerable software
 - V12n logistics as out-of-band attack vector
 - Hypervisor as attack method
- Forensics, malware analysis
 - More convenience for old techniques
 - New techniques emerging

Nightmares

- Breakouts (*attack the hypervisor*)
 - Software in a guest VM causes effects in the host or another VM
 - Subvert interaction features, like cut-and-paste or file sharing
 - Arbitrary code execution... game over!
- Resource hogging (*logistics as vector*)
 - Shared network, disk, memory, CPU resources
 - How about filling up the host's file-system with log entries?
- Blue pills (*V12n as root-kit*)
 - Nested, totally invisible virtualization

Sweet dreams

- Forensics
 - Forensic imaging is a one-click operation
 - Snapshots and replay functionality allow deep inspection
 - Debugging features are a window into guest systems
- VMsafe
 - One VM is designated as “special”
 - API available to operate on other VMs
 - Terremark joins RSA, IBM, Symantec, McAfee and others
 - “...provides fine-grained visibility over virtual machine resources, making it possible to monitor every aspect of the execution of the system...” – vmware.com/go/vmsafe
 - This changes the game for virtual IDS and all the rest.

Agenda

- What v12n is and isn't
- Virtual security hype
- Truly new issues
- **Compliance impact**
- Conclusion

V12n: Convenient compliance

- Some things are more convenient
 - Easily architect n-layer systems with isolated backend networks
 - Deploy standard images with a click
- Some things stay the same
 - Patching, crypto, anything that has nothing to do with v12n
 - Expect evolution here, as researchers find more loopholes
- Some additional best practices
 - Harden the host OS and patch the v12n infrastructure
 - Disable unnecessary v12n features, like cut-and-paste or file sharing
- Defense in depth: assume that access to one VM implies access to all the VMs on the same hardware
 - Treat hardware as a sort of trust boundary
 - Group VMs of a similar security sensitivity together

Agenda

- What v12n is and isn't
- Virtual security hype
- Truly new issues
- Compliance impact
- **Conclusion**

Conclusion

“Any sufficiently advanced technology is indistinguishable from magic.”

- Software that pretends to be hardware
 - It’s cool, but it’s not magic
- A few things are easier
 - New ways to deal with hardware
 - Because really, it’s software, and software is more malleable
- Most things stay the same
 - SQL injection, buffer overflows, social engineering, inside jobs
- A couple of things are new, or newly complicated
 - New ways to attack the hardware
 - Because really, it’s software, and software is more vulnerable