Securing the Virtual Environment: How to Defend the Enterprise Against Attack

Matthew Wallace
Davi Ottenheimer
- Introduction
- Background
- 10 Chapters of Securing the Virtual Environment (Cloud)
- Lessons learned since VMworld 2012
Introduction
Introduction

Matthew Wallace (@mattwallace)

viawest
Cloud | Colocation
Managed Services

Davi Ottenheimer (@daviottenheimer)

flyingpenguin
the poetry of information security
Why Write a Book and Give Presentations?

- Address Resistance to Virtualization and Cloud
- Demystify Security Differences from Physical
- Illustrate Known and Expected Attack Vectors
- Clarify Control Costs for a New Ecosystem
- Guide Compliance and Regulation
Background
General or Specific to Technology?

- **Long-term utility**
  - General principles last. Specifics change
  - Human behavior and technology mix

- **Vendor neutrality**
  - Not intended to be a hardening guide
  - Clouds don’t exist in a vacuum
  - Many sites not 100% virtual or sole-vendor
  - Ecosystems matter

Image: http://fishing.ws/
How to fix it, or what can be broken?

- There are attempts to create standards and help – e.g., Cloud Security Alliance and Cloud Control Matrix
- Best practices for typical controls have been evolving for decades
- Easier to define threats and classes of threats
- Solutions are evolving, but we touch on some of them

Remember this?

Image: http://www.flickr.com/photos/55935853@N00/5847690037/
Big or Small Picture?

- **Systemic Risks**
  - Fire-and-forget. APIs get less eyeballs
  - User provisioning
  - Software-destroyed Datacenter
  - Trusted Root and Certificates

- **Operational Duties**
  - Change, Patch, Change Again
  - Manage Identities
  - Monitor Logs
How Bad Can it Be?

- [IaaS] Cloud Extends and Enhances Virtualization
  - More “self” service
  - More multi-tenancy

- Security Doesn’t Come First

- 90% of some OS infected with malware

- Savings/Utility Drives Business
  - Things Move, Like it or Not (Dropbox, AWS, etc)
  - Avoiding Cloud Isn’t Inherently Safer

https://ssd.eff.org/tech/malware
http://www.neatoshop.com/product/Tentacle-Doorstop
10 Chapters of Securing the Virtual Environment
Virtualization, the Cloud…

“What are the barriers to cloud computing? The top issue overall was a perceived lack of security and service level agreements (SLAs), with 45% of respondents referring to it.”

“…our instruments are open to committing serious errors.”

Jules Verne, 20,000 Leagues Under the Sea
Cloud computing has the potential to be ubiquitous; electrical grid

**Figure 3.** Workload Distribution: 2010 - 2015

*Source: Independent Analyst Shipment Data, Cisco Analysis*
Understanding of cloud IS improving, though

<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>Example responsibility assignment for management of controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Install and maintain a firewall configuration to protect cardholder data</td>
<td>IaaS: Both, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>2: Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>IaaS: Both, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>3: Protect stored cardholder data</td>
<td>IaaS: Both, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>4: Encrypt transmission of cardholder data across open, public networks</td>
<td>IaaS: Client, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>5: Use and regularly update anti-virus software or programs</td>
<td>IaaS: Client, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>6: Develop and maintain secure systems and applications</td>
<td>IaaS: Both, PaaS: Both, SaaS: Both</td>
</tr>
<tr>
<td>7: Restrict access to cardholder data by business need to know</td>
<td>IaaS: Both, PaaS: Both, SaaS: Both</td>
</tr>
<tr>
<td>8: Assign a unique ID to each person with computer access</td>
<td>IaaS: Both, PaaS: Both, SaaS: Both</td>
</tr>
<tr>
<td>9: Restrict physical access to cardholder data</td>
<td>IaaS: CSP, PaaS: CSP, SaaS: CSP</td>
</tr>
<tr>
<td>10: Track and monitor all access to network resources and cardholder data</td>
<td>IaaS: Both, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>11: Regularly test security systems and processes</td>
<td>IaaS: Both, PaaS: Both, SaaS: CSP</td>
</tr>
<tr>
<td>12: Maintain a policy that addresses information security for all personnel</td>
<td>IaaS: Both, PaaS: Both, SaaS: Both</td>
</tr>
</tbody>
</table>

**PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers**

Understanding scope for cloud environments requires looking at both physical and virtual, and providing segmentation on each.
(2) Outsider Attack

- Outsiders not necessarily unknown
- A stolen password away from compromise? (Administrator cloud login->GuestCustomization/Console Access)
- Role Based Access Requires Roles (Underspecialization… Google incident)
- PKI infrastructure is critical but fragile
- Credentials are insufficiently strong
  - Too easy to steal
  - Too “re-usable” (ssh fallback passwords)

"I would never join a club that would have me as a member."

Groucho Marx
(2) Get Visibility

- Log as much as you possibly can
- Log shells in particular (especially ESXi if you have shell logins enabled)
- For Unix infrastructure, consider sshd ForceCommand to stop unauthorized tunnels and running unlogged commands
- Do firewall and log VPN traffic; the typical end-user machine with VPN connectivity combines privileged access with weak security
- Virtualization as a layer of protection for client machines
(2) Updates, Software, and Authentication

- Only install from trusted sources
- Check package signatures
- Pursue two-factor authentication for management tools
- APIs and two-factor are a tricky business
(3) Making the Complex Simple

- **Panacea fixes gone horribly wrong**
  - IDS spinning fans
  - “Awareness” gaps

- **Simple attack vectors**
  - Unprotected wires
  - Weak API, admin interfaces, and orchestration tools

- **Hypervisors have a good track record**

- **Bad practices involve shortcuts….not hard to intercept orchestration tool**
  (vcenter intercept demo)

  “How can you hide from what never goes away?”

  Heraclitus
How often have you ignored a warning?
(4) Denial of Service

- **People, the weak link**
  - Tend to “Go Big”
  - Password choices versus brute force
  - Lockouts = DoS

- **Probing is awfully popular…**
  - Systems with literally no assets or any value other than their processor get thousands of attempts a day
  - Critical infrastructure: “more than 160 in 2011 compared with 9 in 2009”

“I think computer viruses should count as life. Maybe it says something about human nature, that the only form of life we have created so far is purely destructive. Talk about creating life in our own image.”  

Stephen Hawking

http://chinadigitaltimes.net/2007/10/can-a-computer-virus-be-patriotic-zhang-dongfeng/  
(4) Resource constraints – DoS

- **Memory**: drive it over a cliff and watch it crash
- **Disk**: bigger disks are part of the problem
- **Heavy operations**
- **There’s a cloud out there people are “borrowing”** – botnets
- **Shared environment**
  - DoS yourself to DoS your neighbor
  - Quite often, unintentionally
Cloud – Very Shared, Very Proximate

• Shared Resources = Shared DOS
• Even a targeted DOS attack wipes out everything near the target
• Some traditional DDOS protection can only protect the actual DDOS customer
  • Either because their IPs are protected (BGP routes, etc)
  • Or because their content is pre-cached
  • But what about you?

Photo: http://www.flickr.com/photos/yisris/5558550304/
(5) Abusing the Hypervisor

- **Good news** – risk is manageable
- **Bad news** – there are flaws
  - KVM (qemu/PIIX exploit from Nelson Elhage)
  - Cloudburst video driver hack on VMware variants
  - Xen hack via virtual video framebuffer

- **See a pattern? All virtualized devices**

  “Vision is the art of seeing things invisible to others.”
  Jonathan Swift
(5) Demonstrating Risk

- Thomas Edison wanted to “prove” AC dangerous
  - Paid for “stray” cats and dogs to electrocute
  - 1902 “Poison carrots” and electroshock to elephant

- Hypervisor cracks
  - Probably not a good focal point
  - Respond and patch, but don’t panic
  - Log and monitor
  - Protect your endpoints
(5) “VMDK has left the building”

- Purported hypervisor “flaw”
- Requires specially crafted VMDK files
- Verify, don’t trust – high bar for roll your own
- OVF
Hack your system!

- Load “tenant” VMs and try being promiscuous
- Use some inside knowledge
  - Mount iSCSI targets or NFS shares
  - You “shouldn’t” have access (or should need a CHAP secret)
- Port-scan yourself
(5) Automate configuration checks

- Automate config checks to ensure your systems are hardened
  - Configuration manager → NIST SCAP, XCCDF, OVAL
  - Scripts

```bash
vSwitch vSwitch0: OK
vSwitch vSwitch1 [Allows Forged Transmits] [Allows Mac Changes]
Portgroup pgTest100: OK
Portgroup pgTest101: OK
Portgroup pgTest102: OK
Portgroup VM Network: OK
Portgroup vmkernel: OK
Portgroup pgTest103: OK
Portgroup pgTest104: OK
Matts-17:vi_utils matt$
```
(6) Finding Leaks; Obtaining a Side-Channel

Simple or naïve configuration

• Enables easy attack (e.g. MAC address theft)
• Detected by software, in the software-defined datacenter

“Lead me not into temptation; I can find the way myself”

– Rita Mae Brown
(6) PKI Again

- How many vCenter admins used to clicking ignore?
- What would they do in production? (WWTDiP)
- Trained response
  - “Do you want to let windows change your computer…”
  - “I agree to these terms and conditions” button on just about everything
- By the way, your browser trusts the Chinese Ministry of Industry and Information Technology
  - microsoft.com
  - yourdomain.com

(6) Co-tenancy

- Hypervisors safe, but not made of lead
- Easy to know you’re on a VM (Blue Pill)
- Easy to detect host relative to other VM
- Historic attacks relied on proximity
  - Certificate timing attack
  - Classic side-channel attack
  - Observation outside of the cryptosystem
- “Hey, You, Get Off of My Cloud”
  - 2009 paper
  - VM timing keystrokes using side-channels

“These walls are paper thin and everyone hears every little sound”
– Modest Mouse
“Evil events from evil causes spring.”
– Aristophanes
(7) Log Sources

- Keeping up is tough
- No unified format
- Syslog *lip service*

http://nostylgia.wordpress.com/tag/nyc-open-fire-hydrant/
(7) Log Usefulness

- Troubleshooting
- Alerts
- Compliance
- Analysis / Correlation
- Response…

http://nostylgia.wordpress.com/tag/nyc-open-fire-hydrant/
(7) Do you know what your response is? Trigger it.

**Incident Responsiveness**

- **Trigger test**
- **No result =**
  - no plan
  - just hope

---

*What can I help you with?*

*“Siri I'm bleeding really bad can you call me an ambulance”*

*From now on, I’ll call you ‘An Ambulance’. OK?*

- **Cancel**
- **Yes**
“You can’t play a symphony alone; it takes an orchestra to play it.”

– Navjot Singh Sidhu
The good and the bad

- Securing systems can be hard work
- Orchestration tools should make things easier
  - Need credentials to work their magic
  - Add complexity and more attack surface
  - Yet overall reduce cost and human error (or repeat it far more often)

- Common interface
  - Force checks
  - Verify configuration
  - Automate hardening
(7) Use virtualization to automate security!

Conveniently, as we prepared our presentation, William Lam and Alan Renouf published a video and blog on doing exactly this!

(8) Forcing an Interception

- There are a lot of layers, and complexity is dangerous
- API ecosystem – is this a breeding ground for attacks in the future?
- API management, governance, etc, growing market because of this (see: Layer 7, Apigee, etc)

“Complexity is the worst enemy of security” – Bruce Schneier

http://useeit.abc7chicago.com/Media/View/1478781
(8) Network interceptions

- When was the last time you built servers with 10 NICs?
- Still one wire
- Network segregation
  - Service Console
  - vMotion
  - FT
  - Storage
  - Tenant Traffic
- Trust your VLANs?

(9) Abusing SaaS

Not what you might expect – bitten again and again

- File inclusion
- SQL injection (<3 UNION)
- XSRF

“The Past: Our cradle, not our prison; there is danger as well as appeal in its glamour. The past is for inspiration, not limitation, for continuation, not repetition.”

– Israel Zangwill
(9) **SaaSy and pervasive**

- **More and more we rely on this**
  - Dropbox (<3 Octopus)
  - Workday
  - SuccessFactors
  - Gmail, Google Docs
  - Bank Statements, Brokerages, W-2s, E-mail replacing faxes

- **Expected to accelerate**
  - Improved tools for infrastructure and platform layers
  - More projects economically feasible
(10) Building Compliance into Virtual and Cloud Environments

- Compliance Versus Security
- ISO27001/SSAE16
- HIPAA/HITECH
- FedRAMP
- FISMA
- NERC
- PCI
Remember me?

- Segmentation for physical and virtual
- VLANs: yes, they’re “trusted”
- Hypervisors on the bubble of trust

- Understanding scope for cloud environments requires looking at both physical and virtual, and providing segmentation on each.
- Logical segmentation for logical components, physical segmentation for physical components which are not intended to be shared (e.g., IPMI/iLO ports)
Auditors and “guidance”

- There’s a big difference between some firms. And some auditors still had their heads in the sand about virtualization not long ago.

- "could reduce" – Don’t expect completely concrete guidance (yet)

- What is a best practice in the future may vary depending on how well some expected segmentation layers, such as a hypervisor, hold up

- Remember: Virtualization has **PLUSSES** and **MINUSES**; you can add segmentation, auditability, and controls
10 Chapters

1. The Cloud
2. Outsider Attack
3. Make Complex Simple
4. DoS
5. Hypervisor Abuse
6.Leaks and Side-Channel
7. Logs and Orchestration
8. Forcing an Interception
9. Abusing SaaS
10. Compliance
Securing the Virtual Environment: How to Defend the Enterprise – QUESTIONS?

THANK YOU!

@mattwallace
@daviottenheimer