Virtualization

CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu
Administrative

• Homework 4 will be posted today or tomorrow

• Last week of class – project presentations
  – 10-15 minute presentations
  – Turn in slides (PDF or, preferably, PPTX)
    • Must be comprehensive: extra slides not covered in talk should be added to flesh out details
    • Or: optional supporting writeup (PDF)
  – I’ll email about a Doodle to sign up for presentation day/time
Virtualization and cloud security

VMs

Cloud computing paradigms

VM image security issues

VM Introspection

Introspection
Virtualization

No virtualization

Full virtualization

Paravirtualization

Type-1: Hypervisor runs directly on hardware
Virtualization

No virtualization

Full virtualization

Paravirtualization

Type-1: Hypervisor runs directly on hardware
Type-2: Hypervisor runs on host OS
IBM VM/370

• Released in 1972
  – Used with System/370, System/390, zSeries mainframes
  – Full virtualization

• Supported CP/CMS operating system
  – Initial application was to support legacy OS

• z/VM is newer version, most recent version 2010
  – Better use of 64-bit mainframes
Xen

- 2003: academic paper
  - “Xen and the Art of Virtualization”
- Paravirtualization
  - Hypercalls vs system calls
  - Modified guest OS
- Why?
Example VM Use Cases

• Legacy support (e.g., VM/370)
• Development
• Server consolidation
• Cloud computing Infrastructure-as-a-Service
• Sandboxing / containment
Study of malware

• Researchers use VMs to study malware
• Example of VM sandboxing
  – Hypervisor must contain malicious code
• Introspection
• How would you evade analysis as a malware writer?
  – split personalities
VMM Transparency

- Adversary can detect if:
  - Paravirtualization
  - Logical discrepancies
    - Expected CPU behavior vs virtualized
    - Red pill (Store Interrupt Descriptor Table instr)
  - Timing discrepancies
    - Slower use of some resources

Garfinkel et al. “Compatibility is not transparency: VMM Detection Myths and Reality”
Detection of VMWare

MOV EAX,564D5868 <-- "VMXh"
MOV EBX,0
MOV ECX,0A
MOV EDX,5658 <-- "VX"
IN EAX,DX <-- Check for VMWare
CMP EBX,564D5868

IN instruction used by VMWare to facilitate host-to-guest communication

VMWare:
    places VMXh in EBX
Physical:
    processor exception

From
http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf
Server consolidation

• Consolidation
  – Use VMs to optimize use of hardware
  – Pack as many VMs onto each server as possible
  – Turn off other servers

• Threat model?
  – Isolation
  – Containment
  – Assume guests are/can be compromised
Violating isolation

- Covert channels between VMs
  - Illicit communications
  - Hard drives
  - Exploits against VMM
Violating isolation

• Covert channels between VMs
  – Illicit communications
  – Hard drives
  – Exploits against VMM

• Degradation-of-Service attacks
  – Guests might maliciously contend for resources
  – Xen scheduler vulnerability
Violating containment

- **Escape-from-VM**
  - Vulnerability in VMM or host OS (e.g., Dom0)
  - Seemingly rare, but exist

---

**VMware vulnerability allows users to escape virtual environment**

By **Joab Jackson**  ○ Feb 28, 2008

A new vulnerability found in some VMware products allows users to escape their virtual environments and muck about in the host operating system, penetration testing software firm Core Security Technologies **announced** earlier this week.

This vulnerability (CVE Name: CVE-2008-0923) could poise significant risks to enterprise users who are deploying VMware software as a secured environment.
Violating containment

• Escape-from-VM
  – Vulnerability in VMM or host OS (e.g., Dom0)
  – Seemingly rare, but exist

• Side channels
  – Spy on other guest via shared resources
Cross-VM side channels using CPU cache contention

1) Read in a large array (fill CPU cache with attacker data)
2) Busy loop (allow victim to run)
3) Measure time to read large array (the load measurement)

What else is shared? Memory bus, Hard disk, i-Cache, CPU registers, NIC, Hypervisor itself, ...
Lessons

• Don’t count on:
  – VMM transparency
  – Strong isolation (side channels exist)

• Don’t rely on:
  – Containment

• Securing guest OS and host OS still very important
Virtual Machine Management

• Snapshots
  – Volume snapshot / checkpoint
    • persistent storage of VM
    • must boot from storage when resuming snapshot
  – Full snapshot
    • persistent storage and ephemeral storage (memory, register states, caches, etc.)
    • start/resume in between (essentially) arbitrary instructions

• VM image is a file that stores a snapshot
“Protect Against Adware and Spyware: Users protect their PCs against adware, spyware and other malware while browsing the Internet with Firefox in a virtual machine.”

[http://www.vmware.com/company/news/releases/player.html]
VM Management issues

• Reset vulnerabilities
  – We saw crypto/RNG related vulnerabilities a few weeks ago (reuse of randomness)
  – Guest OS and application quiescing

• Lack of diversity

• Identity management / credentials
Amazon Machine Images (AMIs)

- Users set up volume snapshots / checkpoints that can then be run on the Elastic Compute Cloud (EC2)
- Can be marked as public and anyone can use your AMI
5,303 AMIs analyzed (Linux and Windows)


See also Bugiel et al., “AmazonIA: When Elasticity Snaps Back”, 2011
Also: Malware found on a couple AMIs
Balduzzi et al. analysis

• Backdoors
  – AMIs include SSH public keys within authorized_keys
  – Password-based backdoors

<table>
<thead>
<tr>
<th></th>
<th>East</th>
<th>West</th>
<th>EU</th>
<th>Asia</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMIs (%)</td>
<td>34.8</td>
<td>8.4</td>
<td>9.8</td>
<td>6.3</td>
<td>21.8</td>
</tr>
<tr>
<td>With Passwd</td>
<td>67</td>
<td>10</td>
<td>22</td>
<td>2</td>
<td>101</td>
</tr>
<tr>
<td>With SSH keys</td>
<td>794</td>
<td>53</td>
<td>86</td>
<td>32</td>
<td>965</td>
</tr>
<tr>
<td>With Both</td>
<td>71</td>
<td>6</td>
<td>9</td>
<td>4</td>
<td>90</td>
</tr>
<tr>
<td>Superuser Priv.</td>
<td>783</td>
<td>57</td>
<td>105</td>
<td>26</td>
<td>971</td>
</tr>
<tr>
<td>User Priv.</td>
<td>149</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>185</td>
</tr>
</tbody>
</table>

Table 2: Left credentials per AMI
Balduzzi et al. analysis

- Credentials for other systems
  - AWS secret keys (to control EC2 services of an account): 67 found
  - Passwords / secret keys for other systems: 56 found

<table>
<thead>
<tr>
<th>Finding</th>
<th>Total</th>
<th>Image</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon RDS</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>dDNS</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SQL</td>
<td>7</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>MySql</td>
<td>58</td>
<td>45</td>
<td>13</td>
</tr>
<tr>
<td>WebApp</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VNC</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>74</strong></td>
<td><strong>54</strong></td>
<td><strong>20</strong></td>
</tr>
</tbody>
</table>

Table 3: Credentials in history files
Balduzzi et al. analysis

• Deleted files
  – One AMI creation method does block-level copying

<table>
<thead>
<tr>
<th>Type</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home files (/home, /root)</td>
<td>33,011</td>
</tr>
<tr>
<td>Images (min. 800x600)</td>
<td>1,085</td>
</tr>
<tr>
<td>Microsoft Office documents</td>
<td>336</td>
</tr>
<tr>
<td>Amazon AWS certificates and access keys</td>
<td>293</td>
</tr>
<tr>
<td>SSH private keys</td>
<td>232</td>
</tr>
<tr>
<td>PGP/GPG private keys</td>
<td>151</td>
</tr>
<tr>
<td>PDF documents</td>
<td>141</td>
</tr>
<tr>
<td>Password file (/etc/shadow)</td>
<td>106</td>
</tr>
</tbody>
</table>

Table 5: Recovered data from deleted files
“They told me it’s not their concern, they just provide computing power,” Balduzzi says. “It’s like if you upload naked pictures to Facebook. It’s not a good practice, but it’s not Facebook’s problem.”


- Amazon notified customers with vulnerable AMIs
- Made private AMIs of non-responsive customers
- New tutorials for bundling systems
- Working on undelete issues...
Lessons

• New software management practices needed with VM snapshots

• Discussion:
  – New tool support?
  – How much worse is this than non-cloud server deployments?

• We have about ~1600 AMIs downloaded ourselves. Research project ideas?