Trusted Computing & OpenStack

Steve Weis
PrivateCore

OpenStack Security Meetup
July 2014
How safe are bare-metal clouds?

Predictable + elastic + reliable = OnMetal

OnMetal Cloud Servers are single-tenant, bare-metal systems that you can:

- Provision in minutes via an OpenStack® API.
- Mix and match with virtual cloud servers.
- **Pay by the minute**
Attacks in the wild

Shopping for Spy Gear: Catalog Advertises NSA Toolbox
By Jacob Appelbaum, Judith Horchert and Christian Stöcker

Symantec Official Blog
BIOS Threat is Showing up Again!
Created: 09 Sep 2011 10:19:42 GMT • Updated: 23 Jan 2014 18:19:11 GMT

The Register
Malware burrows deep into computer BIOS to escape AV
Exploit all the things!

• Operating Systems
• BIOS / EFI
• Device firmware / Option ROMs
• Master boot records
• Keyboard controllers
• Management engines and controllers
“Provide for the recovery of an information system to a known state”

Source: NIST 800-53
Trusted Execution Technology

Firmware and software needed to boot

Remote Attest

Measure

TPM

CPU

BIOS
Option ROMs
Platform Config
SINIT
Kernel
OS Config
# Example Measurements

<table>
<thead>
<tr>
<th>PCR</th>
<th>Entry Type</th>
<th>Valid</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Final Value</td>
<td>Yes</td>
<td>b21ce8cbe22b63119184908f9b9f5b85e33c78c</td>
</tr>
<tr>
<td>17</td>
<td>Final Value</td>
<td>Yes</td>
<td>fdbfc169c6d6a33f6363686c4e6ff9f8e7f634b0f</td>
</tr>
<tr>
<td>17</td>
<td>SINIT Hash</td>
<td></td>
<td>69ecaace65107595404b7bf48d0728927186e0c4f</td>
</tr>
<tr>
<td>18</td>
<td>Final Value</td>
<td></td>
<td>907511fe2781ed59d28dcd1446721d30602427e0</td>
</tr>
<tr>
<td>18</td>
<td>Kernel Command Line</td>
<td>Yes</td>
<td><code>live_image_url=http://192.168.0.54/fog/public/sweis/auth_keys_filename=auth_keys.cpio.gz static_ip=192.168.0.57 modules_network=bnx2 console=ttys0,115200n8 network_wait_secs=2</code></td>
</tr>
<tr>
<td>18</td>
<td>Tboot Hash</td>
<td>Yes</td>
<td>2da41566d02e5636b3564a9de117f5cc63d18f3c</td>
</tr>
<tr>
<td>18</td>
<td>Tboot Command Line</td>
<td>Yes</td>
<td>logging=serial,vga,memory</td>
</tr>
<tr>
<td>18</td>
<td>Kernel Hash</td>
<td>Yes</td>
<td>f609d8a80a8963f9f74dba167e7eb83b02561a53</td>
</tr>
<tr>
<td>19</td>
<td>Final Value</td>
<td>Yes</td>
<td>ec570d184ee1faeddd88f18c064691bb96322a78</td>
</tr>
<tr>
<td>19</td>
<td>Initrd Hash</td>
<td></td>
<td>52f7b3e74fbd9d42a0bf325b79ee34a4619da4</td>
</tr>
<tr>
<td>23</td>
<td>Final Value</td>
<td></td>
<td>7a863ec6c6136b238c6015a7ab67b5d9e7f0464f</td>
</tr>
<tr>
<td>23</td>
<td>User Certificate</td>
<td>Yes</td>
<td>d36e06de3a1dcc588e2824bb53167d10b73bf574</td>
</tr>
</tbody>
</table>

Displaying 12 items
Gaps in Trusted Execution

- Provenance
- Forge
- Overflow
- BIOS
- Option ROMs
- Platform Config
- SINIT
- Kernel
- OS Config
- TPM
- Hash collision
- Spoof Bus
- Paperclip
- Extract Keys
- CPU
- Spoof CPU

- Past
- Hypothetical
- Current
Attestation in OpenStack
Trusted Compute Pools

1. Run my payload on a trusted compute node
2. Which nodes are trusted?
3. TPM Quote
4. Node A is good
5. Run payload on compute node A
Implementations

- **Open Attestation (OAT)**: [https://01.org/openattestation](https://01.org/openattestation)
  - Open source Java attestation server. Mostly developed by Intel.
- **Intel Trust Attestation Solution** (Mt. Wilson): Enterprise OAT
- **PrivateCore vCage**: Python / Django / Horizon attestation server
Gaps in Trusted Pool Model

Separate Trusted Environment?

Nova  Cinder  Swift  ...  Glance

Attestation Server

Compute Pool

Nova Compute
Nova Compute
Bad Compute

Bad nodes already have control plane access?
Toward a Better Model

1. Attest
2. Authorize
3. Provision
4. Enroll

Trust Perimeter

Attestation Server

Credential Storage

OpenStack Components

Compute Node
Suggested Improvements

1. Attest all servers in OpenStack: Not just compute nodes

2. Cloud providers should provide TPMs and compatible firmware

3. Vendors need to provide authoritative lists of measurement values

4. CPU vendors should ultimately remove dependency on TPMs
Thank you!

Questions?

steve@privatecore.com
@sveis