Standing on the Clouds

A journey in Private Cloud Security
Claudio Criscione - @paradoxengine
SyScan 10
There are a lot of clouds very Fluffy Clouds…
...And less fluffy
A Taxonomy of clouds

Cloud by the book - NIST

On-demand self-service
Broad network access
Resource pooling
Rapid elasticity
Measured Service

Public
Community
Hybrid
Private

Off-Premise
On-Premise

IaaS
PaaS
SaaS
Who plays the game?

XEN – XenCloud
VMware [And the VMware Express players]
Ubuntu – Eucalyptus
Red Hat – DeltaCloud, RHVM
Amazon – Virtual Private Cloud
...and many others
The Road to the Clouds

Market and the technology are both moving toward cloud oriented architectures

Your (new) datacenter is (will be) cloud based

The *build that* syndrome
Quick, go!

We’re rushing forward implementation without really thinking about security.

But wait! I thought security was one of the Big No for cloud implementation!

What about private clouds?
A trojan horse

Private Clouds are the “Trojan horse” of the Cloud Industry

It’s just like standard virtualization!

In the meantime, you get used to those small deltas...
Security Deltas

Management
Semantics
Integration
Network
Management

The “Old Virtualization” Way

1. Hide your management interface
2. Segregate the management network from the internal network
3. Create separated physical management ports

[see vSphere Hardening Guide]

The Private Cloud Way

1. Espose your interface
2. Throw a party to celebrate!
Blackberry strikes back

Last year this guy was managing his XEN farm using a bugged Web Interface with his Blackberry. Now the Blackberry is back on Xen Cloud Platform!

I noticed it was gone as well. You all should correct the security flaws and re-release it. Its an awesome interface, and I can admin my Xen Farm from my Blackberry.

Now the Blackberry is back on Xen Cloud Platform!

critical for me. This means that I have to be able to do most if not all of my admin work from my BlackBerry smartphone. That's the beauty of open source, different focus brings different results.

Whatever anyone feels about it, I won't apologize for writing it because someone has written something similar.

Vern
By the way... introducing VASTO

The Virtualization ASSessment TOolkit

It is an “exploit pack” for Metasploit focusing on virtualization security.

Announcing Beta 0.2 SyScan10 Edition

VASTO now knows some cloud tricks
Shortcuts

Demo Time - 1
Security Deltas

- Management
- Semantics
- Integration
- Network
Integration

Private cloud vendors push for integration with them

“Stock” virtual machines

Management tools

Updates

This way they can make your cloud feel part of a common Sky. However, they should do it securely!
Eating the eucalyptus

Demo Time - 2
Security Deltas

Management

Semantics

Integration

Network
Network

New challenges and old issues

VM Migration
   Even between clouds!
   Still in clear text for most...

Multi tenancy
   Requires (working) network fencing

The whole network stack is a shoot in the dark...
Security Deltas

Management

Integration

Network

Semantics
The Holy Roman Emperor Charles V was once asked which languages he typically used.

"I speak Spanish to God," he explained, "Italian to women, French to men - and German to my horse."

If you want to make it happen, you have to be able to state that

\[
\text{what-the-cloud-undestands} = \text{what-the-cloud-can-do}
\]
Cloud Paradigm

Thou shall not bypass the interface.
Security labeling

We know that “escape from the VM attacks” will happen again.

To mitigate, we can define “zones”

Even if virtualization solutions won’t let us do “host tagging”, admins can do it anyway.

Not with Private cloud computing!
A possible solution

Stating Security Requirements
<table>
<thead>
<tr>
<th>Cloud Solution</th>
<th>Version tested</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eucalyptus</td>
<td>1.6.2</td>
<td>None</td>
</tr>
<tr>
<td>DeltaCloud Portal</td>
<td>0.1.1</td>
<td>Could be</td>
</tr>
<tr>
<td>RHEV</td>
<td>NA – Public APIs</td>
<td>None</td>
</tr>
<tr>
<td>Abiquo</td>
<td>1.5</td>
<td>None</td>
</tr>
<tr>
<td>XEN Cloud Platform</td>
<td>0.1.1</td>
<td>None</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud</td>
<td>NA – March</td>
<td>None (redundancy)</td>
</tr>
<tr>
<td>VMware vCloud Express</td>
<td>NA – March</td>
<td>None</td>
</tr>
<tr>
<td>Svirt-LibVirt</td>
<td>Library source</td>
<td>Partial</td>
</tr>
<tr>
<td>OpenNebula [Haizea]</td>
<td>1.0</td>
<td>Could be</td>
</tr>
</tbody>
</table>
“The limits of your language are the limits of your world”

- Ludwig Wittgenstein
Time to make a stand

As “the security community” it’s our role to make sure that new technologies are not simply taken for granted without a security debate.

Private Cloud is a great risk and a great opportunity

We need to make our voice heard!
One more hack
Off-Premise solutions have to provide

Trust and Security

DO THEY?
What is everyone doing?

HTTP/1.1 200 OK
Server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8g
mod_wsgi/2.6 Python/2.6.2
Vary: Accept-Language,Cookie,Accept-Encoding
Expires: -1
Content-Language: en
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
Content-Length: 114

[["0", ["7810", "$ANYUSERNAME", "COMPLETED", "updateThumbs", "Task completed successfully", "2010/03/22 17:03:35"]]]
(re)Think about your Cloud strategy
You need one!

Check security of outsourcer

Make your voice heard!
Questions
Standing on the Clouds

Claudio Criscione
c.criscione@securenetwork.it
Twitter @paradoxengine
VASTO’s home is at nibblesec.org