A Cloud Security Ghost Story

Craig Balding  cloudsecurity.org
The views and opinions expressed here are those of Craig Balding only and in no way represent the views, positions or opinions - expressed or implied - of my employer or anyone else.
∗ Happy to take questions as we go
∗ Will limit in-flight answers to 2 minutes...
∗ ...to allow time for Q&A at end
∗ If you want SAP Pwnage, other track ;-)
Tweeting/Blogging?

Please add the tag:

cloudsec
Clown Computing?
Cloud == Internet
It’s Outsourcing!
It’s Virtualization!
Overhyped Fad
Nothing New

Don’t Believe in Clouds?
What Is “Cloud”?
Cloud Security vs. Security in the Cloud

Avoid the Facepalm
This is not ASP

- Shared Hardware
- Shared Fabric / Host
- Scalability / Cost

Multi Tenancy
DB Security Model
DB == Tenant
DB == Tenant 1..n
“It’s Only Day 1”
Cloud Magic: Just Say No
Evil State
Replication Woes
Patching Devils
Insidious Integrity
Funding

Cloud FAIL
Risk Management
Your Liable
Compensating Controls
Plan for Failure
Trust but Verify
Web Services Security
Browsers Are Brittle

Security Givens
Ghost Central
*aaS: ...as a Service
Pay As You Go (CC)
Elastic
Outages Very Public
Support Forums

Public Clouds
Classic SPI Model

- Software as a Service
- Platform as a Service
- Infrastructure as a Service
Examples

- Software as a Service
- Platform as a Service
- Infrastructure as a Service
SaaS
CRM
force.com == PaaS
AppExchange
Code Reviews
Service Cloud

Salesforce
Examples

Software as a Service

Platform as a Service

Infrastructure as a Service
Google App Engine

- PaaS
- Python VM
- Justin Ferguson
- Java VM
- Data Import/Export
- SDC
Google Secure Data Connector
Microsoft Azure

- Software & Services
- Technology Preview
- Identity (Cameron)
Software + Services
Examples

- Software as a Service
- Platform as a Service
- Infrastructure as a Service
Public IaaS Pioneer
EC2, S3, SQS etc
“You secure”
Security Whitepaper
Evangelism
Data Cleansing

Amazon Web Services
One Key
Management Plane
New Policy Language
Report a Scan
If a HD is Stolen...
AWS Ecosystem

Amazon Web Services
Dynamo Paper
Consistency
Availability
Integrity
Out of order
No Time Promises

Eventually Consistent
AWS “Dev friendly”
Dev Testimonials
AMZN PMTS
866-216-1072
AWS API endpoints
POST/PUT/DELETE

Developers with Credit Cards
Haunted House of the Cloud

- Visibility
- Mutants
- Cloud Stacks
- Integration
- Privacy
- Regulations
- SLAs
The Visibility Ghost Ship
The Visibility Ghostship

- When Controls Fail
- Lingua Franca: API
- Manage SSL
- EC2 vs NSM
- Immature logging
- DLP
IaaS vs Paas vs SaaS
Scan & Get Canned
Idea: Allow Scan API
Pen-testing Scope

Assurance
Virtual Data Center
Version Control
View as Timeline
Pre/post Commit
Sanity Checks
Proactive Polling
Examining the Virtual Data Center

As a first step, we fetch a representation of the VDC, to ascertain what resources are available and can be created.

To server:

```plaintext
GET /  
Host: xrgy.cloud.sun.com  
Authorization: Basic xxxxxxxxxxxxxxxxxxxxxx  
Accept: application/vnd.com.sun.cloud.compute.Vdc+json  
X-Compute-Client-Specification-Version: 0.1
```

From server:

```plaintext
HTTP/1.1 200 OK  
Content-Type: application/vnd.com.sun.cloud.compute.Vdc+json  
Content-Length: nnn

{
  "name": "XRGY Virtual Data Center",  
  "uri": "http://xrgy.cloud.sun.com\d",  
  "addresses": [
    {
      "name": "144.34.100.199",  
      "uri": "/addresses/144.34.100.199",  
      "ip_address": "144.34.100.199"
    }
  ],  
  "vnets": [
    {
      "name": "vnet1",  
      "uri": "/vnets/10.31.145.0",  
      "netmask": "255.255.255.0",  
      "network": "10.31.145.0"
    }
  ],
}
Incident Response

- Call Premium Support
- Cloud Clamour
- No Business Context
Forensics

- IaaS vs Paas vs SaaS
- Ghosting a Ghost
- Logs & Integration
- Offline Forensic VMs
- AWS EBS Cloning
- Forensics as a Service
- Cloud IR Teams?
IaaS vs Paas vs SaaS
Mash-ups 1...n
Theft of Hard Drive...
First, find the DC
Jurisdictional Hell

Investigations
The March of the Mutated Hypervisor
The March of the Mutated Hypervisor

- AWS EC2
- Xen with “mods”
- No Dom0 Access
- Xen DomU
- Expose via XML API
The Vampire BIOS

- BIOS Functionality++
- Research++
- Cache Snooping
- Hypervisor Attack
- Persistent Rootkits
Ghost in the Stacks
Dependent Services
Consume & Provide
Trust by Inheritance
Mind the Gap
Pass the Buck

Cloud Stacks/Layers
Appirio
Salesforce App
Hook API
Divert Attachments
Client > EC2 > S3
Stored in Plaintext!

Example
How do you make it secure?
Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there it is protected by the same strong security mechanisms that protect thousands of customers using Amazon’s services (see Amazon developer center for more information).

In addition, when sending and receiving data, Appirio uses the Salesforce.com API to confirm that the user belongs to the org they claim to, and that the user has access to the corresponding Salesforce.com record. In addition, because we use the Salesforce.com session object, usage is restricted to users currently logged into Salesforce.com and accessing Salesforce.com records. At no time does Appirio have access to your Salesforce org or data directly.

Please review Appirio’s security and privacy policy for more information.
Enterprise Integration Road to Hell
Identity is > People
Federated Auth
Visibility
DLP
Metrics
Billing

Enterprise Integration
IaaS vs Paas vs SaaS
VM Portability
Frameworks
AWS as defacto API
Unified Cloud?

Interoperability
Cloud Lock-in
The Green Lantern of Privacy
EPIC Compliant
Misstating Security
Snafus & Vulns
Lack of Crypto
Bar of chocolate?
$SOCIALNETWORKS

The Green Lantern of Privacy
The Screaming Regulator
PCI: The Mosso Pitch
HIPAA: AWS / “Apps”
Screaming or silent?
VirtSec / PCI DSS
Groundhog Day

The Screaming Regulator
Legal Concerns

- Jurisdiction
- IP rights
- Content ownership
- Contract Law Wins
- Licensing
- Raid 8
The Curse of the Bloodstained SLA
Blood Stained SLA

No CHANGELOG

Internet == No promises

CC_OK || rm -rf /cloud

Service Credits FTW!

Blood Stained SLA
7.2 We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications.
7.2. ...We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates.
Not even Service Credits? ;-) 

7.2. ...We will have **no liability** to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.
Cloud Nirvana: The Rise of the Enterprise Private Cloud
Private Clouds

- Maximum Control
- Interoperability
- Cloudbursting
- Extend Off-site
- VMware / CISCO
- Eucalyptus (OSS)
<table>
<thead>
<tr>
<th></th>
<th>Managed By(^1)</th>
<th>Infrastructure Owned By(^2)</th>
<th>Infrastructure Located(^3)</th>
<th>Accessible and Consumed By(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
<td>Off-Premise</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Managed</td>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
<td>On-Premise</td>
<td>Trusted &amp; Untrusted</td>
</tr>
<tr>
<td>Private</td>
<td>Organization</td>
<td>Organization</td>
<td>On-Premise &amp; Off-Premise</td>
<td>Trusted</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Both Organization &amp; Third Party Provider</td>
<td>Both Organization &amp; Third Party Provider</td>
<td>Both On-Premise &amp; Off-Premise</td>
<td>Trusted &amp; Untrusted</td>
</tr>
</tbody>
</table>

\(^1\) Management includes: operations, security, compliance, etc...

\(^2\) Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

\(^3\) Infrastructure Location is both physical and relative to an Organization’s management umbrella

\(^4\) Trusted consumers of service are those who are considered part of an organization’s legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Source: Chris Hoff
Enterprise Skeletons

- Infrastructure 1.0
- Firewall Mentality
- Controls vs Data
- Investments vs Risk
- DL Time Bombs
- Visibility & IR
Call from the Grave
Eucalyptus (OSS)
API == AWS EC2
Xen + KVM
Ship w/Ubuntu 9.04

Open Source Private Cloud
Embrace the Cloud

- Centralised Controls
- Password Cracking
- Forensic Readiness
- Never Ending Logs
- Security Builds
- Security Testing
Cloud Aggregator

"Internet Trading Platform"

Public/Private

Handle Billing

Cloud Brokers
Example: Zimory
Gold: A gold SLA cloud delivers the strongest quality standards. This includes availability and security standards. The providers offering these resources are **compliant with all relevant security certifications**.

Silver: A silver SLA offers **high availability and security standards**. The providers are known brands.

Bronze: A bronze SLA delivers the **usual quality** and availability standards of hosting providers. It does not contain certifications and additional security offerings.
Cloud Spirits

**General**
John Willis: IT ESM and Cloud (Droplets)
Kevin L. Jackson: Cloud Musing (Federal)
James Urquhart (CISCO): Wisdom of Clouds
Werner Vogels (AWS CTO): All Things Distributed

**Google Groups**
Cloud Computing

**Security**
Christofer Hoff: rationalsurvivability.com
Craig Balding (aka Me): cloudsecurity.org
Cloud Security Initiatives

- Cloud Security Alliance
- ENISA Cloud Security Working Group
Cloud Security Alliance

- Non-profit organization
- Promote practices to provide security assurance
- Comprised of many subject matter experts from a wide variety disciplines
- Official launch next week @ RSA
- Join? Linkedin Group “Cloud Security Alliance” open to all
ENISA Cloud Computing
Risk Assessment

- European Policymakers responsible for funding Cloud risk mitigation research, policy, economic incentives, legislative measures, awareness-raising initiatives
- Business leaders to evaluate Cloud risks of and possible mitigation strategies.
- Individuals/citizens to evaluate cost/benefit of consumer Cloud services.
Hosting => Cloud
Cloud Platform Wars
Cloud Pwnage
Trust Indicators
Vertical Clouds
Data Centric Security?
Social Engineering++
Ghost Alley / Amsterdam

SPOOK STEEG CENTRUM

Ghost Alley / Amsterdam
Thanks
CSA: Domains

- Information lifecycle management
- Governance and Enterprise Risk Management
- Compliance & Audit
- General Legal
- eDiscovery
- Encryption and Key Mgt
- Identity and Access Mgt
- Storage
- Virtualization
- Application Security

- Portability & Interoperability
- Data Center Operations Management
- Incident Response, Notification, Remediation
- "Traditional" Security impact (business continuity, disaster recovery, physical security)
- Architectural Framework