Pleasant Skies or Gathering Storm: The Good and Evil of Security Services in the Cloud

Adam Goldstein - IT Security Engineer, Dartmouth College
Ryan Speers – Dartmouth Class of 2011, CSI Member, IASP Scholar
Ricky Melgares – Dartmouth Class of 2011, CSI Member

Securing the eCampus - July 28, 2009
Dartmouth Cyber-Security Initiative (CSI)

- The CSI is ongoing collaboration between faculty, staff, and students
- Focused on projects aimed at improving the security of the College's information systems.
- Coordinates research interests with practical concerns
- Student participants in last year:
  - 6 undergraduates (CS and Thayer)
  - 2 Masters students (CS and Thayer)
  - 3 PhD candidates (CS)
Current CSI Projects

- CISCO Critical Information Assurance Group: Network Security Lab
- Public computing and privacy
- PKI Policies in the Enterprise
- “Achilles” Vulnerability Assessment Console
- Netflow profiling and analysis
- Cloud Computing security
Presentation Outline

- Overview
  - Definitions
  - Interest
  - Approach
- Test Process and Findings
- “Mal-Users” in the Cloud
- Risk to Customers
- Recommendations and Next Steps
Cloud Computing - Definitions

- **Software as a Service (SaaS)**
  - Google Apps, Salesforce.com, Hosted MS Exchange
- **Platform as a Service (PaaS)**
  - Google App Engine, MS Azure, Force.com
- **Infrastructure as a Service (IaaS)**
  - Amazon EC2
  - Rackspace Cloud
  - GoGrid
Security Services in the Cloud - Why

- General department interest in researching IaaS (e.g. it’s cheap)
- Many security “services” could be good candidates for the cloud
  - Only needed for a short time
  - Not needed 24/7
  - Not mission-critical
  - Limited sensitive data
# Cloud Pricing (July 2009)

<table>
<thead>
<tr>
<th><strong>Rackspace</strong> : RAM</th>
<th>Hourly</th>
<th>Monthly</th>
</tr>
</thead>
<tbody>
<tr>
<td>256MB</td>
<td>$0.015</td>
<td>$10.95</td>
</tr>
<tr>
<td>512MB</td>
<td>$0.03</td>
<td>$21.90</td>
</tr>
<tr>
<td>1024 MB</td>
<td>$0.06</td>
<td>$43.80</td>
</tr>
<tr>
<td>2048 MB</td>
<td>$0.12</td>
<td>$87.60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Amazon EC2</strong> : RAM/CPUs</th>
<th>Hourly</th>
<th>Monthly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7GB/1</td>
<td>$0.10</td>
<td>$72.00</td>
</tr>
<tr>
<td>1.7GB/5</td>
<td>$0.20</td>
<td>$144.00</td>
</tr>
<tr>
<td>7.5GB/4</td>
<td>$0.40</td>
<td>$288.00</td>
</tr>
<tr>
<td>7GB/20</td>
<td>$0.80</td>
<td>$576.00</td>
</tr>
</tbody>
</table>
Security Services in the Cloud: Examples

- External vulnerability scanning and penetration testing
- External service monitoring
- Application and software evaluation
- Security tool training
- Incident response
Cloud Services – Testing Plan

• Set up accounts for following services
  – Rackspace Cloud
  – Amazon EC2
  – GoGrid

• Tests
  – Scanning
  – Vulnerability Assessment
  – Upload capabilities
Security Services in the Cloud: Acceptable Use Policies

- In general, probing your own systems from the cloud is allowed
- Most AUP’s prevent probing the cloud services without explicit consent from the vendor
Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.

You may make network connections from Amazon EC2 hosted servers to other hosts only with the permission and authorization of the destination hosts and networks. Examples of unacceptable network traffic include:

- Unauthorized probes and port scans for vulnerabilities.
- Unauthorized penetration tests, traffic that circumvents authentication systems or other unauthorized attempts to gain entry into any systems.
Acceptable Use Policies: Testing against the Cloud

• Rackspace AUP:
  “You may not attempt to probe, scan, penetrate or test the vulnerability of a Rackspace Cloud system or network or to breach the Rackspace Cloud's security or authentication measures, whether by passive or intrusive techniques, without the Rackspace Cloud's express written consent.”
Test Findings - Scanning

- Conducted NMAP scans of both Dartmouth Data Centers
- Cloud providers did not block scans or raise alerts on the activity
**Test Findings – Scanning (2)**

- Before whitelisting on our IPS: 801 hosts scanned in 30 seconds
- After whitelisting:
  - /22 subnets (1024 hosts) averaged 35 seconds
  - Max rtt timeout of 100ms produced accurate results
Test Findings – Scanning (3)

- Used scan results to create a “Firewall Map”
- Comparing open ports with flow data to make firewall recommendations
- Internal scanner still needed to test private addresses
Test Findings – Vulnerability Scanning

- Computing Services routinely conducts vulnerability scans from an internal server
- Same scans were conducted from the Cloud
- Again, no blocks or alerts were generated from the vendor
- Exploit tools were also installed on the Cloud servers.
Test Findings – Vulnerability Scanning (2)

- Scan of 200 servers
- Almost 30,000 possible tests per host
- Completed in 6 mins. 56s
Scanning from the Cloud- Cost Analysis

• Current dedicated scanning server: $150/month hardware + additional costs (backup, power, cooling)
• Move to Dartmouth Virtual Machine: $78/month
• Host in the Cloud:
  – Amazon EC2: $12/month
  – RackSpace Cloud: $7.20/month
Testing – Upload Capabilities

• Interested in using the Cloud for incident response and digital forensics
  – Processing power
  – Scalable
  – Only pay as-needed

• Tested upload capabilities of Cloud services

• 250 kbps was best we achieved

• Inadequate for drive image uploads
Gathering Storm?

If the Cloud can be used for good, can it also be used for evil?
Appeal of the Cloud to “Mal-users”

• Why use the Cloud for malicious computing?
  – Cheap
  – Powerful
  – Temporary systems
  – With fraud an increasing motivator of “mal-users”, less skill or interest in compromising systems
  – Anonymous?
Access to the Cloud

- Only a valid credit card and e-mail address are required to set up a cloud server.
- Servers are controlled via web-console and SSH. Easy to access through Tor or an anonymizer
- Stealing Amazon credentials can allow a mal-user to set up Cloud servers.
Cheap Power

- Using own equipment for processor intensive tasks is likely cost prohibitive
- Amazon EC2 High-CPU Extra Large Instance
  - 7 GB of memory
  - 20 CPUs
  - 1690 GB of instance storage
  - Price: $0.80 per instance hour
Minimal Technical Controls

• From our testing, no security controls on what can be run in the cloud
• Received no warnings for scanning, vulnerability probes, or exploits
Risks to Customers - IP addressing

- Filtering/blacklisting
  - Attacks from the cloud to your network?
  - Will it be hard to detect or block attacks from popular cloud services?
  - Will you be blocked if other hosts in cloud are creating problems?
“You may not share or publish Amazon Machine Images ("AMIs") or other content or applications on the AWS Website that are intended to cause, or have the consequence of causing, the user to be in violation of the terms and conditions of this Agreement.”
Risks to Customers – Denial of Service

- No control of inbound filtering to cloud servers
- Some AUP’s state that a server can be blocked if under attack
- From GoGrid AUP:
  “GoGrid may also disable Customer's service if GoGrid suspects that such service is the target of an attack or in any way interferes with services provided to other customers, even if Customer is not at fault.”
- Will scans or other probes against a cloud server be enough to have the provider block it?
Risks to customers – Limited security auditing

- Again, some AUPs prohibit performing security tests against cloud servers
- Minimal understanding of back-end security
  - What can cloud companies access?
  - What controls do they have in place? (HR, Auditing)
Risks to customers – Data retention/e-discovery

- No published policies on how Cloud providers handle e-discovery requests
- What remains when server or storage is deleted?
- Do Cloud providers perform their own backups? What is their retention policy?
- Do providers collect and retain access logs?
Risks to customers – Administrative Console

- Providers use a web-based admin console to control server instances
- Console accounts username/password
- Doesn’t matter how well you lock down servers if attacker can get console credentials
  - Phishing/spearfishing
  - Sharing credentials
  - Guessing
  - Sniffing
Conclusions

- Pleasant skies:
  - Very attractive cost
  - Easy to use
  - Example services
    - Classroom projects/training
    - Test or pilot servers
    - Development systems for low security projects
    - System monitoring and external testing
  - How many systems in your data center could be replaced?
Conclusions – Gathering Storm

- Our recommendations
  - Cloud servers not to be used for any sensitive data
  - Not to be used for mission critical services
  - Not as cost-effective for 24/7 services
  - Institutional Cloud server policy needed
  - Server administration standards needed
  - Monitor Intrusion Prevention Systems for Cloud IP’s
Next steps for CSI Cloud research

- Work with Cloud providers to perform security assessment of Cloud hosting environment
- Further “upload” testing with Cloud storage services
- Research e-discovery in the cloud
Thanks!

Adam Goldstein
IT Security Engineer
Peter Kiewit Computing Services
Adam.goldstein@dartmouth.edu

Ryan Speers – Dartmouth 2011
Ricky Melgares – Dartmouth 2011