ISACA Presentation

Cloud, Forensics and Cloud Forensics
Agenda

- What is the Cloud
- What is Forensics
- Challenges Cloud poses to Information Security and Forensic Investigations
- Using Cloud technologies to support investigations and forensics
- Risks – Control, Compromise and Chain of Custody
Understanding the Audience

• By a show of hands - how many people know what the cloud is?
• How many people know what a virtual machine is?
• How many people know what software as a service is?
• How many people know what computer forensics is?
What is the Cloud

• Simply – a datacenter infrastructure maintained by a third party that delivers on-demand virtual computing, platform and application services
Types of Cloud Computing
Spectrum of the Cloud

Cloud Computing Service Models

- **Software as a Service (SaaS)**: End-user applications delivered as a service, rather than on-premises software.
- **Data as a Service (DaaS)**: Data provided as a service rather than needing to be loaded and prepared on-premises.
- **Platform as a Service (PaaS)**: Application platform or middleware as a service on which developers can build and deploy custom applications.
- **Infrastructure as a Service (IaaS)**: Compute, storage or other IT infrastructure as a service, rather than as dedicated capability.
Examples

The Cloud Spectrum

**IaaS**
- Amazon
- GoGrid
- Linode
- Rackspace
- Others...

**PaaS**
- AppEngine
- Azure
- EngineYard
- Force.com
- Heroku

**SaaS**
- Google Apps
- Salesforce
- Taleo, Workday, many, many more...

Cloud Strategies
Experts on the Business of Cloud Computing
Cloud - Internal, Private, Public
## Advantages and Disadvantages

### Advantages

1. **Cost** – Transform Capital Expenditure for servers into and operating expense.
2. **Multi-tenancy** – Several customers share the same infrastructure.
3. **Scalability** – “On-demand” provisioning of computing resources.
4. **Redundancy** – Redundancy of sites is easier to implement.
5. **Accessibility** – Device and location independence.
6. **Maintenance** – Upgrades are applied centrally and done by IT experts.

### Disadvantages

1. **Security** – Loss of control over sensitive data.
2. **Dependency** – Tied to you Cloud Service Provider.
3. **Flexibility** – Special customization of computing resources may not be possible.
4. **Cost** – Cost structure is becoming opaque.
5. **Knowledge** – Most knowledge is concentrated at the Cloud Service Provider.
6. **Integration** – Difficult integration with other equipment and systems.
Compliance Concerns

• Numerous regulations pertain to the storage and use of data,
  – Payment Card Industry Data Security Standard (PCI DSS),
  – the Health Insurance Portability and Accountability Act (HIPAA),
  – the Sarbanes-Oxley Act, among others.

• Many of these regulations require regular reporting and audit trails. Cloud providers must enable their customers to comply appropriately with these regulations.
Security and Compliance Planning

• **Business continuity and data recovery**
  – Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered. These plans are shared with and reviewed by their customers.

• **Logs and audit trails**
  – In addition to producing logs and [audit trails](#), cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., [eDiscovery](#)).

• **Unique compliance requirements**
  – In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.\textsuperscript{[14]}
Cloud Security

• Cloud Security Alliance - largest and arguably most comprehensive player in cloud security standards
• NIST - http://www.nist.gov/itl/csd/cloud-012412.cfm
• IEEE – project P2301, Guide for Cloud Portability and Interoperability Profiles,
• **Beware SAS 70** - has already seen its light fade in world of cloud services
# Obstacles and Opportunities

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Availability of Service</td>
<td>Use Multiple Cloud Providers; Use Elasticity to Prevent DDOS</td>
</tr>
<tr>
<td>2 Data Lock-In</td>
<td>Standardize APIs; Compatible SW to enable Surge Computing</td>
</tr>
<tr>
<td>3 Data Confidentiality and Auditability</td>
<td>Deploy Encryption, VLANs, Firewalls; Geographical Data Storage</td>
</tr>
<tr>
<td>4 Data Transfer Bottlenecks</td>
<td>FedExing Disks; Data Backup/Archival; Higher BW Switches</td>
</tr>
<tr>
<td>5 Performance Unpredictability</td>
<td>Improved VM Support; Flash Memory; Gang Schedule VMs</td>
</tr>
<tr>
<td>6 Scalable Storage</td>
<td>Invent Scalable Store</td>
</tr>
<tr>
<td>7 Bugs in Large Distributed Systems</td>
<td>Invent Debugger that relies on Distributed VMs</td>
</tr>
<tr>
<td>8 Scaling Quickly</td>
<td>Invent Auto-Scaler that relies on ML; Snapshots for Conservation</td>
</tr>
<tr>
<td>9 Reputation Fate Sharing</td>
<td>Offer reputation-guarding services like those for email</td>
</tr>
<tr>
<td>10 Software Licensing</td>
<td>Pay-for-use licenses; Bulk use sales</td>
</tr>
</tbody>
</table>
What is Computer Forensics

• Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

• The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.
Lab Based Forensics

• Forensics has traditionally been a lab based practice

• Media copied and examined directly
Case Study Over Time

• Imagine you had an employee suspected of stealing company information and you are a forensic examiner assigned to investigate the electronic media.

• Fifteen years ago, that meant you were on a plane!
Traditional Best Practice

Suspect

Read

Read/Write

Forensic Copy

Hash Verification 100% Match
Chain of Custody and Evidence Protection
2003 to Present? - Enterprise Network Acquisition

Suspect

Read

Hash Algorithm | Hash Result
--- | ---
MD2 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
MD4 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
MD5 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
SHA-1 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
SHA-224 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
SHA-384 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em
SHA-512 | 38 5f 0f 42 3e 7a 85 20 85 ea b9 7c 38 ed of 09 3d 81 ae de 14 04 81 24 ff 5a 45 e3 2f in Em

Hash Verification 100% Match

Read/Write

Forensic Copy
A physical safe has been replaced by - Network Area Storage
What Affect Does the **Private** Cloud Have On Forensics
Personal Device, Virtual Image, Server Host– Evidence Collection
What Affect Does the **Private** Cloud Have On Forensics

Suspect

Forensic Copy

Hash Verification
100% Match
What Affect Does the **Public** Cloud Have On Forensics

BYOD, Virtual Image, Server Host– Evidence Collection
Effects on InfoSec and Investigations

• Information Security
  – Control and Ownership Data
    • Insider Threat - Espionage, Theft, Access
    • External Threat - Provider compromise
    • Provider hostage – nickel and dime fees

• Investigations
  – No access to hardware, hard drives, etc
  – Limited access Virtual Machines
  – Personal device – Consent required.
  – No covert investigation capability without Law Enforcement or Subpoena
Recommendations

• We are in the midst of the largest technical evolution in a couple decades

• Read up on current Cloud security standards, start small but definitely start. Get your feet wet if you're not already swimming

• Choose a Hybrid between Internal and private cloud.

• Design and control the VM’s used by your company

• Install advanced monitoring tools into the VM Image – may be better for evidence than traditional forensics
Recommendations

• Monitor or block access to Cloud instances not managed by your company – Hold off on BYOC for a while (Bring your own Cloud)
• Be careful doing BYOD and Cloud at the same time
• The FILE is the new PERIMETER –
  – Information Rights Management: has its time come?
  – DLP?
• The cloud is inevitable, it just makes sense. Don’t fight it, just use good judgment and move at the right pace
Forensics as a Service

- Using a combination of IaaS, DaaS and SaaS, a forensic infrastructure could be designed to be cloud based.
  - Instant Virtual Lab, set up anywhere, anytime
  - Snapshot and replicate machines for very powerful cracking capability
  - Scale up for large processing or eDiscovery jobs
  - Pay for what you use

- So VERY different from where we were 15 years ago!
Thank You

• Thoughts? Questions?
Credits

- [http://www.comparethecloud.net/cloud-computing/#types](http://www.comparethecloud.net/cloud-computing/#types)
- [www.Logicube.com](http://www.Logicube.com)