Cloud Breach - Forensics Audit Planning

GOALS

• Why it is more complex to answer:
  - Who, what, when, where & how (security analytics)

• Service level Agreements (SLA)

• Aid your cloud-computing security audit planning
Your CIO hears from the CEO and CFO. The FBI is investigating why your next billion $$ pharmaceutical cancer drug is on-line.

This confidential information was found on the servers of a global Cloud Service provider exposed and unprotected.
1. Cloud Architecture Overview
2. Cloud Forensics
   a. Forensic Data Sources
      a. logging
      b. Trusted Data
      c. Virtual Machines
      d. Federated (shared) Services
      e. Cloud Brokers
3. Cloud Service Providers
   a. Dropbox
   b. SalesForce.com / Force.com
   c. Amazon.com Web Services
4. Cloud Anti Forensics
5. Summary
Cloud Service Architecture

- Application
  - Monitoring
  - Content
  - Collaboration
  - Communication
  - Finance

- Platform
  - Object Storage
  - Identity
  - Runtime
  - Queue
  - Database

- Infrastructure
  - Compute
  - Block Storage
  - Network
Cloud Service Architecture

Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Clouds
Cloud Service Architecture

Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud

Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
Cloud Service Architecture

- **Deployment Models**
  - Private Cloud
  - Community Cloud
  - Public Cloud

- **Service Models**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

- **Essential Characteristics**
  - On Demand Self-Service
    - Broad Network Access
    - Resource Pooling
  - Rapid Elasticity
  - Measured Service
Cloud Service Architecture

Deployment Models
- Private Cloud
- Community Cloud
- Public Cloud

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Essential Characteristics
- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

Common Characteristics
- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

© 2011 Cloud Security Alliance, Inc. All rights reserved.
Cloud Service Architecture (shared responsibility)

Figure 1—Cloud Service Models

IaaS
Infrastructure as a Service
- APIs
- Core Connectivity and Delivery
- Abstraction
- Hardware
- Facilities

PaaS
Platform as a Service
- Integration and Middleware
- APIs
- Core Connectivity and Delivery
- Abstraction
- Hardware
- Facilities

SaaS
Software as a Service
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content

Source: Universal Model, © Cloud Security Alliance. Used with permission.
Cloud Breach
Forensic Data Sources

- Access logs
- API Management logs
- Security logs (firewall, IDS, opensource tools, etc.)
- Billing records
- Metadata - application
- Netflow, Packet Capture
- Physical drives
- Virtual drives
- Guest OS data
- Cloud data storage
- Certificate and private Keys
Cloud Breach Forensics

Forensics Process Flow

Figure 2. Three different cloud deployment models

Identification

Evidence Identification

Collection

Examination

Organization

Analysis

Presentation
Cloud Forensics
Logs Issues

- Decentralization of logs
- Volatility of logs
- Multiple tiers and layers
- Archival and retention
- Accessibility of logs
- Non existence of logs
- Absence of critical information in logs
- Non compatible / random log formats

- Cloud Application Logging for Forensics (Raffael Marty, 2011)
Cloud Forensic Data

<table>
<thead>
<tr>
<th>Layer</th>
<th>Cloud Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Guest Application</td>
</tr>
<tr>
<td>5</td>
<td>Guest OS</td>
</tr>
<tr>
<td>4</td>
<td>Virtualization</td>
</tr>
<tr>
<td>3</td>
<td>Host OS</td>
</tr>
<tr>
<td>2</td>
<td>Physical Hardware</td>
</tr>
<tr>
<td>1</td>
<td>Network</td>
</tr>
</tbody>
</table>

Trust - definition:
Forensically sound in consideration of the evidentiary integrity of the electronically stored information (ESI)
Cloud Forensic Data

<table>
<thead>
<tr>
<th>Layer</th>
<th>Cloud Layer</th>
<th>Acquisition Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Guest Application</td>
<td>Depends on data</td>
</tr>
<tr>
<td>5</td>
<td>Guest OS</td>
<td>Remote forensic software</td>
</tr>
<tr>
<td>4</td>
<td>Virtualization</td>
<td>Introspection</td>
</tr>
<tr>
<td>3</td>
<td>Host OS</td>
<td>Access virtual disk</td>
</tr>
<tr>
<td>2</td>
<td>Physical Hardware</td>
<td>Access physical disks</td>
</tr>
<tr>
<td>1</td>
<td>Network</td>
<td>Packet capture</td>
</tr>
</tbody>
</table>

**Trust - definition:**

Forensically sound in consideration of the evidentiary integrity of the electronically stored information (ESI)
## Cloud Forensic Data

<table>
<thead>
<tr>
<th>Layer</th>
<th>Cloud Layer</th>
<th>Acquisition Method</th>
<th>Cloud Trust required</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Guest Application</td>
<td>Depends on data</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>5</td>
<td>Guest OS</td>
<td>Remote forensic software</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>4</td>
<td>Virtualization</td>
<td>Introspection</td>
<td>HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>3</td>
<td>Host OS</td>
<td>Access virtual disk</td>
<td>Host, Hardware, Network</td>
</tr>
<tr>
<td>2</td>
<td>Physical Hardware</td>
<td>Access physical disks</td>
<td>Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>Network</td>
<td>Packet capture</td>
<td>Network</td>
</tr>
</tbody>
</table>

**Trust** - definition:
Forensically sound in consideration of the evidentiary integrity of the electronically stored information (ESI)
Cloud Forensic Data

Virtual Machine (VM) IaaS

- **Image Mounting**
  - Encase Physical Disk Emulator
  - Mount Image Pro
  - Paraben P2 Explorer

- **VM Configuration**
  - LiveView
  - Virtual Forensics Computing
  - ProDiscover
  - Other GUI and Command Line Based Tools

- **Virtual Applications**
  - VMware Player, Server, Workstation
  - Other virtual applications
Cloud Forensic Data (IaaS)

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Tool</th>
<th>Evidence Collected</th>
<th>Time (hrs)</th>
<th>Trust Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EnCase</td>
<td>Success</td>
<td>12</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>FTK</td>
<td>Success</td>
<td>12</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>FTK Imager (disk)</td>
<td>Success</td>
<td>12</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>Fastdump</td>
<td>Success</td>
<td>2</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>Memoryze</td>
<td>Success</td>
<td>2</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>FTK Imager (memory)</td>
<td>Success</td>
<td>2</td>
<td>OS, HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>1</td>
<td>Volume Block Copy</td>
<td>Success</td>
<td>14</td>
<td>OS (imaging machine), HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>2</td>
<td>Agent Injection</td>
<td>Success</td>
<td>1</td>
<td>HV, Host, Hardware, Network</td>
</tr>
<tr>
<td>3</td>
<td>AWS Export</td>
<td>Success</td>
<td>120</td>
<td>AWS Technician, Technician’s Host, Hardware and Software, AWS Hardware, AWS Software</td>
</tr>
</tbody>
</table>

J. Dykstra and A. T. Sherman, 2012 - Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing:

Forensic evidence tools & the time to retrieve the data and trust requirements - Amazon Web Services (AWS) EC2 components
Cloud Forensic Data
VM Snapshot
Cloud Forensic Data

VM Hypervisor Types - 1 & 2
Cloud Forensic Data
VM Commercial Hypervisors

KVM is used by Redhat Enterprise Virtualization (RHEV).

Xen Server hypervisor by Citrix Inc.

VMware Inc. vSphere uses VMware’s ESXi hypervisor.

Hyper-V is a commercial hypervisor provided by Microsoft.
Cloud Forensic Data

Federated (shared) Storage
Cloud Forensic Data
Federated (shared) Services

Cloud Services Syndication Value Chain

Disintermediation Potential:
(e.g. a business subscribes to Salesforce.com or QuickBooks.com)
Cloud Forensic Data
Cloud Brokers

NIST SP 500-292 (Cloud Brokers)

Manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

("Adds value" – Gartner Research)
Cloud Brokers
(maturity model)

Identifying Next Steps for Your Cloud Journey

NIST SP 500-292 (Cloud Brokers)

Manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
## Cloud Breach - Forensics Audit Planning

### Issues:

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location independence</td>
<td>Discovery of computational structure</td>
</tr>
<tr>
<td></td>
<td>Legal jurisdiction</td>
</tr>
<tr>
<td>Rapid elasticity</td>
<td>Evidence preservation</td>
</tr>
<tr>
<td></td>
<td>Data integrity</td>
</tr>
<tr>
<td>Data reliability (replication)</td>
<td>Chain of custody</td>
</tr>
<tr>
<td></td>
<td>Evidence integrity</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>Attribution of data</td>
</tr>
<tr>
<td></td>
<td>Chain of custody</td>
</tr>
<tr>
<td>General, abstract data structures</td>
<td>Best evidence</td>
</tr>
<tr>
<td></td>
<td>Presentation/Visualization of evidence</td>
</tr>
</tbody>
</table>
Cloud Services Providers

- "Application" Cloud (SaaS)
  - Builds on "Service" Cloud
  - "Service" Cloud (Web Services, Components)
    - Builds on "Infrastructure" Cloud
      - "Infrastructure" Cloud (Network, Compute, Storage, Middleware)
Cloud Services Providers
Dropbox Security Services

Encryption at rest and in transit

Your files are stored using 256-bit AES encryption, and SSL creates a secure tunnel for data transfers.

Remote wipe

If a computer is lost or someone leaves your business, remotely delete the Dropbox folder to keep your business's most important data safe. BETA

Two-step verification

Add an additional layer of security by securing Dropbox accounts with a password and a phone.

Privacy

Our privacy policy is designed to safeguard the collection, use, and disclosure of your team's information.

Certifications and compliance

Dropbox's storage is SSAE16/SOC1, SOC2, ISAE 3402 and ISO 27001 certified on Amazon S3 and may provide data mirroring across other secure data centers.

Reliability

Keep your work safe with storage designed for 99.999999999% durability.
Cloud Services Providers

salesforce™
Single Sign-On Implementation Guide

Single Sign-On: SAML Assertion (3\textsuperscript{rd} Party)

* Delegated Authentication Single Sign-On

* MS Active Directory, IBM, HP, Ping Identity, NetIQ, etc.,
Cloud Services Providers

Salesforce.com as Identity Provider

User initiates login

Sends response to service provider

Service Provider

Identifies user

Authenticates certificate if necessary

Enables login

1. User tries to access a service provider already defined in Salesforce.
2. Salesforce sends a SAML response to the service provider.
3. Service provider identifies the user and authenticates the certificate.
Cloud Services Providers

**Force.com - Software Developers**

**Separation of duties:**

- Authentication, Authorization, Accounting and Auditing
- Role-based Access Control (RBAC)
- User Access Reviews (logs)

**API management**  - (Mashery, Intel, etc.,)

**Key & Certificate Management**  - (Venafi, Entrust, Comodo, etc.,)
## Cloud Services Providers

<table>
<thead>
<tr>
<th>SaaS Solutions</th>
<th>A5 Cloud Services</th>
<th>Etherios: Expert Cloud Consulting Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fujitsu</td>
<td>No Rating</td>
<td>6 stars</td>
</tr>
<tr>
<td>CloudSteer Technology Pte Ltd</td>
<td>Kandisa Technologies</td>
<td>Dell Services</td>
</tr>
<tr>
<td>3 stars</td>
<td>1 star</td>
<td>1 star</td>
</tr>
<tr>
<td>4 stars</td>
<td>2 stars</td>
<td>1 star</td>
</tr>
<tr>
<td>Basati</td>
<td>Davanti Consulting Salesforce.com services</td>
<td>Wipro Consulting Partner</td>
</tr>
<tr>
<td>3 stars</td>
<td>No Rating</td>
<td>1 star</td>
</tr>
</tbody>
</table>

[https://appexchange.salesforce.com](https://appexchange.salesforce.com)
Cloud Services Providers

Amazon Web Services
Amazon Simple Storage Service (S3)

Cloud Services Providers

AWS Shared Responsibility Model for Infrastructure Services

Figure 1: Shared Responsibility Model for Infrastructure Services
Cloud Services Providers

AWS Audit Security Tips

- Limited access to administrative ports to only a few IP addresses
- ports 22 (SSH), 3389 (RDP), and 5500 (VNC).

- Limited access to common database ports:
  - 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

- **Identity & Access Management** is configured to help ensure secure access control of AWS resources.
  - **Multi-factor authentication (MFA)** token is enabled to provide two-factor authentication for API (Ruby, .NET, Python, PHP, etc.,) access to the root AWS account.

**Access keys** are used to digitally sign API calls made to AWS services. Each access key credential is comprised of an access key ID and a secret key.
Cloud Services Providers

AWS Audit Security Tips

Identity Access Management

- MS Active Directory, LDAP, Kerberos integration

- Single Sign On / Identity Federation
  - CA CloudMinder, SailPoint, Okta, OneLogin, Ping Identity, etc.,

- Role Based Access Controls
  - Assign permissions to groups, not users.

- Administrators should have individual accounts
Cloud Services Providers

AWS Shared Responsibility Model for Container Services

Example: Amazon RDS for Oracle is a managed database service in which AWS manages all container layers including the Oracle database platform.
Cloud Services Providers

AWS Cloud Trail

- Logs any action performed via the APIs or web console into an S3 storage bucket or Glacier archiving storage

- Gives complete audit trail of all changes in your account.

- Set up the S3 (storage) bucket with versioning to prevent tampering of your logs

- Analyzed by Splunk, Sumo Logic, etc.

- can add AWS CloudWatch API activity
Cloud Services Providers
AWS Cloud Trail – use case

Vodafone Australia - Elastic Compute Cloud (EC2)

- Trend Micro Inc. and Xceedium, Inc.'s Xsuite with Amazon’s native security groups
- Set up multiple virtual private clouds (VPC),
- A separate VPC for security tools
- Trend Micro’s Deep Security tool, integrated with AWS APIs, for centralized visibility into the VPCs
Cloud Services Providers

AWS Shared Responsibility Model for Abstracted (Storage) Services

- Amazon S3 and Amazon DynamoDB - AWS operates the infrastructure layer, the operating system, and platform

- Customer uses their devices to store and retrieve data for business uses
Cloud Services Providers

Amazon CloudWatch

Monitors API activity and delivers log files

Developers / system administrators to collect and track metrics,

Monitors Amazon EC2 and Amazon RDS DB instances system wide (Zones East, West, Ireland, etc.,)

Programs retrieve your monitoring data, view graphs, and set alarms, spot trends

Take automated action based on the state of your cloud environment.
Cloud Anti Forensics

Critical - Time to detect and react to an incident
- earlier in attack chain, less loss, less damage, & more forensic evidence

● Cyber criminals remove audit trail, logs. ...
Cloud Anti Forensics

- Denial of Service (DoS / DDoS)
- Destroy Virtual machine (server / application)
- Destroy virtual storage
- Hide virtual infrastructure - routers, switches, (turn off)
- Corrupt forensic data
  - Hashes, certificates, keys
  - Timestamps (NTP)
  - File signatures
- Logs deleted
- Hypervisor security manipulated
Key Issues in Cloud Forensics

1. Acquisition of data is more difficult
2. Cooperation from cloud providers is paramount.
3. Cloud data may lack key forensic attributes.
4. Current forensic tools are unprepared to process cloud data.
5. Chain of custody is more complex.
Join the Fight?

Valdez Ladd, MBA – ISM, CISA, CISSP, www.linkedin.com/in/valdezlad
“Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data.”

Major Issues:

**Architecture** (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.)

**Data collection** (e.g., data integrity, data recovery, data location, imaging, etc.)

**Analysis** (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.)

**Incident first responders** (e.g., trustworthiness of cloud providers, response time, reconstruction, etc.)

**Role management** (e.g., data owners, identity management, users, access control, etc.)

**Legal** (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.)

**Standards** (e.g., standard operating procedures, interoperability, testing, validation, etc.)

**Training** (e.g., forensic investigators, cloud providers, qualification, certification, etc.)

**Anti-forensics** (e.g., obfuscation, data hiding, malware, etc.)
The identification, collection, and preservation of media can be particularly challenging in a cloud computing environment given several possible factors, including:

1) **Identification of the cloud provider and its partners.** This is needed to better understand the environment and thus address the factors below.
2) **The ability to conclusively identify the proper accounts** held within the cloud by a consumer, especially if different cyber personas are used.
3) The ability of the forensics examiner to **gain access to the desired media.**
4) **Obtaining assistance of the CSP** : cloud infrastructure/application provider service staff.
5) Understanding **the topology, proprietary policies, and storage system** within the cloud.
6) Once access is obtained, the examiner’s ability to **complete a forensically sound image of the media.**
7) The sheer **volume of data** with the storage media.
8) The ability to **respond in a timely fashion** to **more than one physical location** if necessary.
9) **E-discovery, log file collection and privacy rights** given a multi-tenancy system. (How does one collect the set of log files applicable for this matter versus extraneous information with possible privacy rights protections?)
10) **Validation of the forensic image.**
11) The ability to **perform analysis on encrypted data** and the collector’s **ability to obtain keys** for decryption. The storage system no longer being local. There is often no way to link given evidence to a particular suspect other than by relying on the cloud provider’s word.

*** FBI, other US Government has agreements with many major cloud service providers and use "National Security Letters" to obtain access without warrant and / or legal warrants veted by a judge.

Prepared by the NIST Cloud Computing Forensic Science Working Group, the report summarizes a staggering 65 challenges cloud computing presents to forensics investigators who sift through bits and bytes of digital evidence to solve crimes.

The challenges are technical, legal and organizational.
References

Image: Cloud Forensics Process Flow, slides 11, 25

Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems

Image: Virtual Machine Quinescence, slide 17

Investigating the Implications of Virtual Machine Introspection for Digital Forensics

Citation


*** Copyrights handled in accordance with “Fair Use” for educational purposes ***
References

Image – slide 17  Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Amazon.com web services

J.Dykstra and A. T. Sherman,  April 2012

Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques
Josiah Dykstra and Alan T. Sherman,


Cyber Defense Lab, Department of CSEE
University of Maryland, Baltimore County (UMBC)

*** Copyrights handled in accordance with “Fair Use” for educational purposes ***