Forensics in the Cloud

Faculty:
Scott Greene
of Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

Cloud Based Digital Forensics

Fun Facts You Should Know

- RockYou.com was hacked in 2009
- An examination of the 32 million compromised passwords and found that tens of thousands of users relied on terrible passwords.
- The password “123456” took first place with 290,731 hits
- “12345,” “123456789,” “Password” and “iloveyou” rounded out the top five most-used passwords.

Types of Cloud Services

- Software as a service (SaaS)
  - SaaS typically entails:
    - Users using a web browser to access:
      - Office applications
      - Messaging software
      - DBMS software
      - Management software
      - Accounting
      - Collaboration
      - CRM
      - HRM
      - Help Desk
Types of Cloud Services

- **Platform as a Service (PaaS)**
  - These providers are usually just providing a server and perhaps an Operating System.
  - These may include limited applications like:
    - Execution Runtime
    - Database servers
    - Web servers

Types of Cloud Services

- **Infrastructure as a Service (IaaS)**
  - Typically only
    - Virtual machines
    - Servers
    - Storage

Types of Cloud Services

- **Private cloud**
  - Private cloud is cloud infrastructure operated solely for a single organization.
  - Private clouds may be internally or externally managed.
**Types of Cloud Services**

- **Public cloud**
  - Public clouds are the services rendered over a network that is open for public use.
  - Public cloud services may be free or offered on a pay-per-usage model.
  - There is not much difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources).
  - Communications over a public network need to be encrypted.
  - Public cloud service providers include: Amazon AWS, Microsoft and Google.

- **Community cloud**
  - Community cloud shares a common infrastructure between several organizations from a specific community with common concerns.
  - A group of agencies for instance.

- **Hybrid cloud**
  - Hybrid cloud is a composition of two or more clouds (private, community or public).
  - Each piece is distinct but they are bound together, offering the benefits of multiple deployment models.
  - Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.
  - Gartner defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers.
Cloud Contract Items to Consider

- E-discovery:
  - Organizations need to have a handle on how E-discovery will be handled:
    - All data stored in a Provider's environment must be available for e-discovery.
    - How will it be located, preserved, collected, processed, reviewed and produced.

Legalities of Cloud Technology

- Preservation / Litigation Hold
  - What is it?
  - Why is it?
Cloud Contract Items to Consider

- **Freedom of Information Act:**
  - In the case of governmental agencies, how will FOIA (or their equivalent) requests be handled?

Cloud Blended Forensics

- **Growth of data**
  - As cloud services are growing, so is the average size of a digital forensics case. The estimated growth rate is 35% per year. Not a small amount. The average in 2003 was 83 GB; the average in 2007 was estimated to be 277 GB.
  - Evidence Solutions, regularly processes 5 to 10 TB cases.
  - The result is that the amount of forensic data that must be processed exceeds the ability to process it in a timely manner.
Cloud Blended Forensics

- Data is stored in the cloud but likely originated elsewhere.
  - Cell Phones
  - Computers
  - Cars and Trucks
  - Other Systems

Cloud Blended Forensics

- Technical Challenges
  - You (likely) can't show up and image a hard disk drive
  - Much of what we collect is from live systems – live forensics

Cloud Forensics

- Process - Cloud:
  - Identify
  - Label
  - Collect
  - Includes Client Side Artifacts
Cloud Forensics

- Resource Pooling Complications
- Saves $$$
- Complicates collection and preservation

Cloud Forensics

- Metadata in the cloud
- Authentication
- Access Control
- Object – Level Accesses

Cloud Forensics

- Metadata in Cloud Forensics
- Firewall ( if any )
- Access logs ( if any )
Cloud Forensics

- Inter – Dependencies
- Investigate chains
  - Who created the data
  - How did it get here
  - Where did it go
- Coordination of responsibilities among all parties / custodians

Cloud Forensics – Key Players

- Investigators - Internal
  - Internal investigators are responsible for investigating misconduct.
  - Work with Law Enforcement (LEOs)
  - Need to have investigative skills
  - Need to have overview of cloud assets

- Other IT professionals
  - System & Network Professionals
  - Ethical Hackers (White Hat)
  - Security Professionals
  - Technical and Support Staff
Cloud Forensics – Key Players

- Legal Advisors
  - Key Key Key
  - Confidentiality
  - Privileged Communications
  - Legal Ramifications
    - Help Prevent breaking the law during an investigation
    - SLA Confirmation / Contractual Requirements
    - Jurisdictional Issues

Cloud Forensics – Key Players

- Legal Advisors
  - Interact or direct interaction with LEOs
  - Direct Collaboration with LEOs
  - Communication
    - Between entities
    - Public Relations

Cloud Forensics – Key Players

- Internal Incident Handlers
  - Should have a concept of how to preserve evidence
  - Interact with external investigators
  - Manage written incident handling plans
Cloud Forensics – Key Players

- Internal Incident Handlers
  + Have knowledge of:
    - Malicious code: Viruses, Trojans, Etc
    - DDOS
    - Tenant’s Confidentiality
    - Data leakage
    - Data Loss
    - Unauthorized Data Access

Cloud Forensics – Key Players

- External Investigators
  + Can come up to speed quickly on Architecture
  + Can review and advise on relevant:
    - Policies
    - Procedures
    - Plans
    - Actions

Cloud Forensics – Key Players

- External Investigators
  + Can be more readily relied upon for interaction with LEOs
  + Can be ready to Testify (Deposition & Court Room)
  + Are more likely to be seen as independent
    - (Especially when the culprit is an insider)
  + Are objective
Denial Of Service (DOS)
- Denial of service attacks are a significant threat.
- The assault by hundreds of thousands or millions of automated requests must be dealt with before it ties up operations.
- It is becoming more difficult to deal with DOS as attackers have become sophisticated and attacks are distributed (DDOS)
- Which makes it harder to detect legitimate traffic.

Cloud Security Threats
- For cloud customers, a sophisticated DDOS attack is like being caught in Austin rush-hour traffic; there's no way to get to your destination, and nothing you can do about it.
- A DDOS attack can shut down your cloud services
- You may be paying for the resources consumed during the attack.
Malicious Insiders

- Insiders with an axe to grind can be a significant problem.
- Malicious insiders aren’t a common threat.
- Background checks can help.

Cloud Security Threats - Malicious Insiders

Prevention:
- Keep your encryption keys on premises, not in the cloud.
- Stand ready to deny access to individuals if the need arises.

Abuse Of Cloud Services

- With Cloud computing it might take an attacker years to crack an encryption key.
- But using an array of cloud servers, he might be able to crack it in minutes.
- Cybercriminals might use cloud servers to serve malware, launch DDoS attacks, or distribute pirated software.
Cloud Security Threats

Abuse of Cloud Services
- Responsibility for cloud services rests with service providers.
- How do they detect inappropriate uses?
- Do they have a clear definition of what constitutes abuse?
- How will they react if it occurs?
- Cloud customers need to assess service provider behavior to see how effectively they respond.

Cloud Security Threats

Insufficient Due Diligence
- Take your time implementing cloud services.
- Do your due diligence.
- You must understand what the service provider has in the way of their environment and protections.
- What will they do in response to an incident?
- What encryption do they provide?
- What security monitoring do they provide?

Insufficient Due Diligence
- As a customer you must know these things.
- Not knowing exposes your organization to increased frustration and risks that you won't find until it is too late.
Cloud Security Threats

Insufficient Due Diligence
- Don't let mismatched expectations between customer and service exist.
- What are the contractual obligations for each party?
- How is liability to be divided?
- How transparent is the service provider?
- What kind of customer service should you expect?

Cloud Security Threats

Insufficient Due Diligence
- You are pushing applications with internal on-premises security controls to the cloud.
- If these are not clearly defined…
- You don't have network controls in the cloud
- You must understand the security environment of the cloud.

Cloud Security Threats

Shared Technology
- Unless you negotiate different, you are in a multi-tenant environment
- A single compromise of a single component, such as the hypervisor, can expose your data along with every one else’s.
- This can affect all kinds of shared services, including CPU caches, shared database services, or shared storage.
Cloud Security Threats

Shared Technology
- The cloud is shared infrastructure, and a misconfigured provider’s operating system or application can lead to compromises.
- You must have an in-depth defensive strategy.
- This strategy must apply to: use of computing power, storage, networking, applications, and user access.
- You should be able to monitor these and should watch for destructive moves and behaviors.

Cloud Based Digital Forensics

Just Because it’s the Cloud

Remember to:
- Require Strong Passwords Locally & in the cloud.
- Don’t re-use passwords
- Ensure your data is backed up
I value your comments. Please fill in your evaluation form found at the end of your packet.

Scott Greene, SCFE
Evidence Solutions, Inc.
866-795-7166
Scott@EvidenceSolutions.com