CLOUD FORENSICS: AN OVERVIEW

Kumiko Ogawa
What is Cloud Forensics

- Forensic Science
  - Application of science to the criminal and civil laws that are enforced by police agencies in a criminal justice system.
- The application of digital forensic science in cloud computing models
Cloud Crime

- **Target**
  - DoS attack

- **Subject**
  - Unauthorized modification
  - Deletion of data
  - Identity theft of users

- **Tool**
  - Botnet
  - Proxy server
Case example

- Amazon EC2
  - Amazon EC2 was compromised and password-stealing trojan had infected client computers. (Dec 2009)
    (http://news.cnet.com/8301-1009_3-10413951-83.html)

- Investigation to CSP, Crydon Technology
  - March 2009
    - FBI seized computer servers belonging to a cloud computing service provider for an investigation into VoIP fraud
    - 50 companies were put out of business

- Web mail
  - Search warrant to CSP
Cloud Forensics

- Traditional approaches to evidence collection and recovery are no longer practical

- We need to establish the procedure
Ref:

Cloud forensics: An overview (Jan 2011)

by Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie
Three dimensions of cloud forensics

- Technical Dimension
- Organizational Dimension
- Legal dimension
Technical Dimension

- Private cloud / Public cloud
  - Cloud infrastructure is owned by CSP in Public cloud

- IaaS / PaaS / SaaS
  - In the SaaS model, the customer does not obtain any control
  - The customers do not have any chance to analyze potential incidences

Technical Challenges of Forensic Investigations in Cloud Computing Environments (Jan 2011) by Dominik Birk
Technical Challenges in Forensic data collection

- SaaS customers may have little to no access to data required for a forensic investigation.

- Many CSPs do not provide services or interfaces for the customers to gather forensic data, e.g. IP logs.
Technical Challenges in Elastic, static and live forensics

- The proliferation of endpoints
  - e.g. mobile
- Unification of log
  - Timestamps
  - Log formats
- Recovered deleted data
  - Some deleted data might be still present in the snapshot after deletion
Technical Challenge in Evidence segregation

- Audit logs of shared resources and other forensic data are shared.
- Some resources e.g. CPU are not designed for strong compartmentalization in a multi-tenant architecture.
- Investigation without breaching the confidentiality of other tenants.
Technical Challenges in virtualized environments

- Tools and procedures are yet to be developed for investigations in virtualized environment

- Lack of policies, procedures and techniques on hypervisor level to facilitate investigation

- How to analyze the image?
Organizational Dimension

- Organizational structure for each cloud organization
  - IT Professionals, Incident Handlers, Legal Advisor

- Chain of Dependencies
  - CSPs and most cloud applications often have dependencies on other CSP(s).
Organizational Challenges regarding SLA

- Important terms regarding forensic investigations are not included in the SLA

- Most cloud customers are still not aware of the potential issues
Legal dimension

- Multi-jurisdiction
  - Data centers are deployed around the world

- Multi-tenancy
  - Service Level Agreement
Legal Challenges regarding Multi-Jurisdiction and multi-tenancy

- What kind of data can be accessed and retrieved
- How to retrieve evidence without breaching privacy or privilege rights of tenants
- What kind of chain of custody is needed
Opportunities

- Data abundance
  - when a request to delete a cloud resource is made it actually technically can never result in true wiping of the data

- Overall Robustness
  - Automatically generated hash
  - on-demand cloning of virtual machines
  - snapshot
Ref:

Cloud forensics: An overview (Jan 2011)

by Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie