Cloud Forensics Challenges

NIST Cloud Computing Forensic Science Working Group

NIST Cloud Forensics Workshop
NIST Gaithersburg, MD
March 24, 2014

<table>
<thead>
<tr>
<th>A. Michael Salim</th>
<th>Dr. Keyun Ruan</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTO, ADTI / LocalWeb.com</td>
<td>Senior R&amp;D Scientist, Espion Ltd.</td>
</tr>
</tbody>
</table>
Contributors

- Keyun Ruan
- Mike Salim
- Josiah Dykstra
- Kenneth Zatyko
- Bob Jackson
- Lon Gowen
- Ernesto Rojas
- Laura Taylor
- Scot Reemelin
- Ken Stavinoha

- Karla Holm
- Kristy Westphal
- Tony Rutkowski
- Fred Cohen
- Nancy Landreville
- Anil Karmel
- Pw Carey
- Mark Potter
- Ragib Hasan
NCC-FSWG - Who We are

• NIST Working Group, Established in November 2012
• Voluntary Open Membership
• Active participants meet bi-weekly by conference call
  – Cloud Forensics Practitioners
  – Cloud Providers
  – Academia
  – US Government User Community
  – International Participants
  – Chaired by NIST (Co-chairs Dr. Michaela Iorga and Eric Simmon, and Dr. Martin Herman, NIST Senior Advisor).

• About 190 members in mailing list, with about 8-10 active bi-weekly participants.

• Twiki Website: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics
NCC-FSWG - Goals

• Gather Inputs
• Identify and aggregate published cloud forensic challenges
• Analyze and prioritize Cloud Forensics Challenges

Tentative goals, may evolve over time:
• Prioritize the challenge categories
  – Based on importance, urgency
  – Based on whether solutions involve technology, standards, or measurements components
• Choose the highest priority challenges and determine gaps in technology, standards and measurements to address these challenges
• Develop a roadmap to address these gaps
NCC-FSWG – Current Status

• Developed USG Survey, will be sent out in near future.
• Challenge spreadsheet – aggregation of published challenges and analysis
• White Paper describing preliminary analysis of Cloud Forensic challenges – progress report
Cloud Computing Forensic Science Challenges

• White paper
• Work In Progress
• First draft almost complete and will be released very shortly for public comments
• Authored collectively by NCC-FSWG bi-weekly participants over the past 18 months.
Cloud Computing Forensic Science Challenges

• Cloud challenges accumulated from a variety of sources and references over time.
• Aggregation and analysis of accumulated challenges.
• Analysis of forensics stakeholder roles and cloud actors.
• Analysis of Cloud Computing Forensic Science challenges.
<table>
<thead>
<tr>
<th>Short Title</th>
<th>Challenge</th>
<th>Normalized [FORMULA]: For a [actor/stakeholder (e.g., consumer)], [action/operation] applicable to [object of this action] is challenging because [reason]</th>
<th>Primary Category (Subcategory)</th>
<th>Related Category (Subcategory)</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletion in the cloud</td>
<td>Deletion in the cloud</td>
<td>For forensic examiners, identifying and attributing data that is deleted in the cloud to a specific user is a challenge because the sheer volume of data and users constantly operating in a cloud environment limits the amount of backups that the cloud service provider will retain. AND/OR For forensic examiners, identifying and attributing data that is deleted in the cloud to a specific user is a challenge because cloud service providers may not implement sufficient methods for retaining information on deleted data in an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) delivery models.</td>
<td>Architecture</td>
<td>Data Collection (Data Recovery)</td>
<td>REF39</td>
</tr>
<tr>
<td>Recovering overwritten data</td>
<td>Recovery of deleted data that is overwritten by another user in a shared virtual environment [Change to, “Recovery of deleted data before it may be overwritten.”]</td>
<td>For all stakeholders, recovering deleted data that is overwritten by another user is a challenge because in a shared virtual environment, there may not be a snapshot in time (e.g., backup) or other record that contains an image of the data before it was overwritten.</td>
<td>Architecture</td>
<td>Data Collection (Data Recovery)</td>
<td>REF2, REF1, REF15, REF23</td>
</tr>
<tr>
<td>Evidence correlation</td>
<td>Evidence correlation</td>
<td>For investigators, correlation of activity is a challenge because there is no interoperability between CSPs.</td>
<td>Analysis</td>
<td>N/A</td>
<td>REF2, REF1, REF14, REF22</td>
</tr>
<tr>
<td>Reconstructing virtual storage</td>
<td>Liability and reconstruction of virtual storage in cloud environments from physical disk images</td>
<td>For all investigators and courts, reconstruction of virtual images or storage is challenging because these reconstruction algorithms need to be validated or developed.</td>
<td>Analysis</td>
<td>Incident First Responders (Reconstruction)</td>
<td>REF2, REF3, REF15</td>
</tr>
<tr>
<td>Timestamp synchronization</td>
<td>Synchronization of timestamps</td>
<td>For analysts, correlating the observable with disparate timestamps is challenging because timestamps may be inconsistent between many</td>
<td>Analysis</td>
<td>N/A</td>
<td>REF40, REF1, REF2, REF4, REF5, REF8</td>
</tr>
</tbody>
</table>
Cloud Computing Forensic Science Challenges

• Accumulation of challenges
  – Gathered in spreadsheet, 60-70 challenges
  – List still evolving, therefore not comprehensive
  – Quickly realized that descriptions varied widely between sources, leading to ambiguity.
  – Developed a “Normalized” schema for describing Cloud Computing Forensic challenges.
Cloud Computing Forensic Science Challenges

Normalized challenge [formula]:
For an [actor/stakeholder], [action/operation] applicable to [object of this action] is challenging because [reason]
Cloud Computing Forensic Science Challenges

• Once challenges were normalized, the list was pruned for:
  • Duplications
  • Not specific to Cloud nor exacerbated by the Cloud
  • Ambiguous challenges

• Literature review: References provided for these challenges (100+)
Cloud Computing Forensic Science Challenges

• Patterns of aggregation began to emerge:

  • Architecture related challenges
  • Data collection challenges
  • Challenges to the analysis of cloud forensic data
  • Anti-forensic challenges
  • Incident first responders challenges
  • Challenges related to role management
  • Legal challenges
  • Challenges related to standards
  • Challenges related to training
Architecture

• E.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc. Architecture challenges in cloud forensics include dealing with variability in cloud architectures between providers; tenant data compartmentalization and isolation during resource provisioning; proliferation of system, locations and endpoints that can store data; accurate and secure provenance for maintaining and preserving chain of custody; infrastructure to support seizure of cloud resources without disrupting other tenants etc.
Data Collection

• E.g., data integrity, data recovery, data location, imaging, etc. Data collection challenges in cloud forensics include locating forensic artifacts in large, distributed and dynamic systems; locating and collecting volatile data; data collection from virtual machines; data integrity in a multi-tenant environment where data are shared among multiple computers in multiple locations and accessible by multiple parties; inability to image all the forensic artifacts in the cloud; accessing the data of one tenant without breaching the confidentiality of other tenants; recovery of deleted data in a shared and distributed virtual environment; etc.
Analysis

• E.g., Correlation, reconstruction, time synchronization, logs, metadata, timelines, etc. Analysis challenges in cloud forensics include correlation of forensic artifacts across and within cloud providers; reconstruction of events from virtual images or storage; integrity of metadata; timeline analysis of log data including synchronization of timestamps; etc.
Anti-forensics

• E.g., obfuscation, data hiding, malware, etc. Anti-forensics are a set of techniques used specifically to prevent or mislead forensic analysis. Challenges in cloud forensics include the use of obfuscation, malware, data hiding, or other techniques to compromise the integrity of evidence; malware may circumvent virtual machine isolation methods; etc.
Incident first responders

- E.g., trustworthiness of cloud providers, response time, reconstruction, etc. Incident first responder challenges in cloud forensics include confidence, competence, and trustworthiness of the cloud providers to act as first-responders and perform data collection, difficulty in performing initial triage and processing a large volume of forensic artifacts collected; etc.
Role Management

• E.g., data owners, identity management, users, access control, etc. Role management challenges in cloud forensics include uniquely identifying the owner of an account; decoupling between cloud user credentials and physical users; ease of anonymity and creating fictitious identities online; determining exact ownership of data; authentication and access control; etc.
Legal

- E.g., Jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc. Legal challenges in cloud forensics include identifying and addressing issues of jurisdictions for legal access to data; lack of effective channels for international communication and cooperation during an investigation; data acquisition that relies on the cooperation of cloud providers, as well as their competence and trustworthiness; missing terms in contracts and service level agreements; issuing subpoenas without knowledge of the physical location of data; seizure and confiscation of cloud resources may interrupt business continuity of other tenants; etc.
Standards

• E.g., SOPs, interoperability, testing, validation, etc. Standards challenges in cloud forensics include lack of even minimum/basic standard operating procedures, practices, and tools; lack of interoperability among cloud providers; lack of test and validation procedures; etc.
Training

• E.g, forensic investigators, cloud providers, qualification, certification, etc. Training challenges in cloud forensics include misuse of digital forensic training materials that are not applicable to cloud forensics; lack of cloud forensic training and expertise for both investigators and instructors; limited knowledge by record-keeping personnel in cloud providers about evidence; etc.
Cloud Computing Forensic Science Challenges

• Stakeholders and Actors
  – Cloud Actors
    • *Per NIST Cloud Computing Security Reference Architecture*
    • Consumer, Provider, Broker, Auditor, Carrier
  – Cloud Forensic Stakeholders
    • *Not so well defined*
    • Personal user, enterprise user
    • Cloud Vendors
    • Forensic Investigator
    • Law enforcement
    • Courts
    • Academic Organizations
    • Many others
Cloud Computing Forensic Science Challenges

- Aggregation led to Mind Map
  - Visual representation of
  - Groups of challenges
  - Relationships between challenges
  - Categories and sub-categories of challenges
Cloud Computing Forensic Science Challenges – Mindmap (RELATED)

3/31/2014 4:58 PM
Cloud Computing Forensic Science Challenges – Complete Mindmap
Cloud Computing Forensic Science Challenges – Future WG Activity

• Publish White Paper Draft for public comment in next few days.
• Use Cases.
• Taxonomy.
• 2:15pm session: “Next Steps in Cloud Forensics”, Dr. Josiah Dykstra and WG member panelists.
Cloud Computing Forensic Science Challenges

QUESTIONS?

Dr. Keyun Ruan – sci@ruankeyun.com
Mike Salim – msalim@localweb.com
NIST Working Group Twiki web site: