Cloud Forensics: an Overview

Keyun Ruan
Center for Cyber Crime Investigation
University College Dublin
Co-authors

• Mark Crosbie, IBM Ireland
• Joshua James, University College Dublin
• Ibrahim Baggili (PhD), Zayed University, UAE
• Prof. Joe Carthy, University College Dublin
• Prof. Tahar Kechadi, University College Dublin

Funding

• The Irish Research Council for Science, Engineering & Technology (IRCSET)
• The European Aeronautic Defence and Space Company N.V. (EADS)
DIGITAL INVESTIGATION IN THE CLOUD
• Global interconnection, openness and interoperability
• Safe havens
• Modern consumer, business, political, scientific, and educational activities will be powered by cloud computing
• Cybercrime (105 billion) > Drug dealing
• Law enforcement not catching up
• “To avoid breaches, the good guys have to succeed 100% of the time. The bad guys only have to succeed once”
"States must identify and prosecute cyber criminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner."

International Strategy for Cyberspace, May 2011
What happened and what is happening in the Cloud?
CLOUD FORENSICS IS MULTI-DIMENSIONAL
**Technical Dimension**

- Chain of custody
  - Admissibility
- Soundness
  - Transport
- Storage
  - Destroy
- Case management

---

**Preservation**

**Collection**
- (Media)
  - Pro-active
  - Client-side
  - Provider-side
  - Data sources
  - Mobile endpoints
  - Physical locations
  - Sampling
  - Time sync
  - ...

**Examination**
- (Data)
  - Evidence segregation
  - Traceability
  - Filtering
  - Pattern matching
  - Data reduction
  - ...

**Analysis**
- (Information)
  - Data mining
  - Reconstruction
  - Time sequence
  - ...

**Reporting**
- (Evidence)
  - Documentation
  - Presentation
  - Expert testimony
5 main areas of focus

• Forensic data collection
• Elastic, static & live forensic toolkits
• Evidence segregation
• Investigative tools in virtualized environments
• Pro-active preparations
3 main areas of focus

• Segregation of duties
• Collaboration
• Policy
Legal Dimension

• Multi-jurisdiction
• Multi-tenancy
• Multi-ownership
• Service Level Agreement
WHAT DO EXPERTS SAY?
Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability

- Launched 13th Feb 2011
- 156 responses up to 23rd Mar 2011
- 192 responses up to now
50%: CLOUD MAKES FORENSICS HARDER

- Loss of data control
- No access to physical infrastructure
- Legal issues of multi-jurisdiction
- Multi-tenancy and multi-ownership
- Lack of tools for larger-scale distributed and virtualized systems
- No standard interfaces
- No provider cooperation
- Difficulties in producing forensically sound and admissible evidence in court
More computing resources and processing power with reduced cost
Rapidly scalable auditing, reporting, and testing analysis can be used for larger datasets and distributed applications
Forensic implementations and activities can be centrally administered and managed
Investigations can be provided as a service by the CSP

42%: CLOUD MAKES FORENSICS EASIER
Technical Dimension 84%
Legal Dimension 84%
Organizational Dimension 75%
TOP 5 CHALLENGES
Investigating external chain of dependencies of the cloud provider: 86.12%

Lack of international collaboration and legislative mechanism in cross-nation data access and exchange: 84.72%

Lack of law/regulation and law advisory: 82.94%

Decreased access to and control over forensic data at all levels from customer side: 79.17%
TOP 3 OPPORTUNITIES
Establishment of a foundation of standards and policies 59.72%

Forensics-as-a-Cloud-Service 57.14%

Cost-effective forensic implementations as part of cloud infrastructure 53.52%
TOP 3 MOST VALUABLE RESEARCH DIRECTIONS
Designing forensic architecture for the Cloud 88.57%
Extending current investigative tools into the Cloud 82.86%
Law 82.2%
TOP 5 MOST NEEDED TOOLS AND PROCEDURES
A procedure and a set of toolkits to:

- Preserve the soundness of digital evidence: 89.55%
- Retrieve forensic data involving confidential data under jurisdiction(s) and agreement(s) under which services are operating: 87.87%
- Investigate external chain of dependencies: 85.07%
- Preserve volatile data: 83.58%
- Proactively collect forensic data: 83.58%
SERVICE LEVEL AGREEMENT
<table>
<thead>
<tr>
<th>Access to Forensic Data</th>
<th>Technical Dimension</th>
<th>Organizational Dimension</th>
<th>Legal Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Encryption keys</td>
<td>• Proactive preparation</td>
<td>• Staffing structure</td>
<td>• Multi-jurisdiction</td>
</tr>
<tr>
<td>• Logs on all levels</td>
<td>• Forensic data collection</td>
<td>• Forensic training</td>
<td>• Multi-tenancy</td>
</tr>
<tr>
<td>• Physical location/physical infrastructure</td>
<td>• Transparency of data collection</td>
<td>• Collaboration</td>
<td>• Chain of custody</td>
</tr>
<tr>
<td>• Disk images and other forensic data generated</td>
<td>• Forensic tools</td>
<td>• External assistance</td>
<td>• Notification</td>
</tr>
<tr>
<td>• Pro-active forensic data collection</td>
<td>• Evidence segregation</td>
<td>• Transparency on chain of dependencies</td>
<td>• Resource seizure</td>
</tr>
<tr>
<td></td>
<td>• Virtual environment and hypervisor investigation</td>
<td></td>
<td>• Forensic soundness</td>
</tr>
<tr>
<td></td>
<td>• Data deletion</td>
<td></td>
<td>• Evidence admissibility</td>
</tr>
<tr>
<td></td>
<td>• Incident response &amp; recovery</td>
<td></td>
<td>• Change of CSP</td>
</tr>
</tbody>
</table>

**Auditing**
CLOUD FORENSICS CAPABILITY MODEL
Initiatives
COLLECTIVE KNOWLEDGE

• Cybercrime and Cloud Forensics: Applications for Investigative Processes. Vol. 1 Vol. 2
• Cloud Forensics Network
• e-Journal of Cloud Forensics Research, UCD CCI

CASE STUDIES

TOOL DEVELOPMENT

BENCHMARK PROJECT

STANDARD & SLA

MY DISSERTATION
Thank You!

Q&A

keyun.ruan@ucd.ie