Forensics-as-a-Service and Models for Forensic Brokerage

Dr. Keyun Ruan
University College Dublin
What is Cloud Forensics?

• Law enforcement perspective
• Security perspective
• Traditional digital forensic challenges
• Digital forensics in the cloud ecosystem
Organizational Challenges

- Split of control
- Segregation of duties
- Chain of dependencies
- Lack of transparency

Source: NIST 500-292 Cloud Computing Reference Architecture
Technical Challenges


Source: NIST SP 500-292
Technical Challenges

• Hybrid forensic acquisition
• Evidence segregation
• Instance isolation
• Time synchronization
• Data integrity

• Identity and anonymity
• E-discovery
• Proliferation of endpoints
• Encryption
• Interoperability
• ...

Legal Challenges

• Multi Jurisdiction
• Multi Tenancy
• Data Ownership
• Privacy
• Service Level Agreement
Survey Results

- 257 respondents
- Proposed definition: “Cloud Forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.

Opportunities for Cloud Forensics

Dedicated forensic implementations are more cost-effective when applied on a larger scale and offered as part of the cloud infrastructure

Establishment of a foundation of standards and policies for forensics that will evolve together with the technology

Forensics-as-a-Servive (using cloud computing to deliver forensic services)

The scalability and flexibility of the Cloud enables elastic and unlimited storage of logs and increases efficiency of indexing, searching and various queries of logs, etc.

Default technologies provided in the Cloud such as automatic MD5 checksums can improve the overall robustness of forensics in the Cloud

There are more chances to find critical evidence left in the Cloud due to data abundance

Cloud Forensic Investigative Architecture

FaaS and Cloud Brokerage

- Single consistent interface
- Business broker, technical broker, or both
- Aggregation
- Arbitrage
- Intermediation

Source: NIST SP 500-292
Models for Cloud Forensic Brokerage

Key Features:
- Elasticity
- FaaS
- Big data/analytics
- Standard Interface

- Broker for Investigative Capability
- Broker for Investigative Process
- Broker for Investigative Toolkit
Key Takeaways

- Cloud forensics poses significant challenges in organizational, technical and legal dimensions
- Definition of cloud forensics
- There are opportunities to be leveraged for cloud forensics including FaaS and standardization acceleration
- Cloud Forensic Investigative Architecture
- Models for cloud forensic brokerage
My Book

- Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, December 2012: http://www.igi-global.com/book/cybercrime-cloud-forensics/69206
Questions?
Thank you!

- @ruankeyun
- keyun.ruan@ucd.ie
- www.cloudforensicsresearch.org