Plenary Session 2: Cloud forensics musts

Cloud Forensics musts for LI/RD Compliance

Tony Rutkowski, mailto:tony@yaanatech.com
EVP, Standards & Regulatory Affairs
ETSI TC LI Rapporteur for Cloud LI

©2014 Yaana Technologies, LLC. All Rights Reserved.
The Cloud LI/RD Initiative

- DTR101567 & 101566 started in TC/LI June 2011 after LI/RD Elements paper in Feb 2011
  - Lawful Interception (CLI) and Retained Data (CRD) needs and requirements in the converged cloud/virtual service environment
  - Challenges and obstacles of complying with those requirements
  - What implementations can be achieved under existing LI/RD standards
  - What new work may be required to achieve needed Lawful Interception capabilities

- Included extensive industry organization activity and systems surveys

- TC/LI is the principal global venue for LI/RD requirements and standards
  - Mobile LI specifications are done in 3GPP SA3LI
Architecture - cloud/virtual service LI challenges

- End-user control
- Support for large number of apps
- Autonomous encryption

- Autonomous access
- Encrypted transport
- High bandwidths
- Now virtualized as NFV/SDN in clouds

- Location Identifier Separation Protocol addresses augment IPv4/6

Cloud resource management, i.e., knowing the location of data and processes among clouds

- Discovering target identities
- App “decoding”
- Autonomous communication with end-user
- Adequate information assurance

Cyber Observable expressions acquired for LI handover
The evolving Technical Report

1. Scope
2. References
3. Definitions and abbreviations
4. Cloud/Virtual Services Overview
5. Lawful Interception Requirements (significant emphasis on mobile)
6. Legacy LI models and methods applied to the Cloud environment
7. [Lawful Interception virtualization]
8. Security in the Cloud LI environment
9. Conclusions and Recommendations

Annex A  Use cases
Annex B  Cloud Virtualization Fora
Annex C  Use Case Guide
Annex D  Use Case Matrix

This clause included virtual forensics tools in the cloud for use on non-cloud and cloud services. TC LI work has been deferred now V0.3.0 (2014-01)
Emerging forensic needs

- Inclusion of forensics for Network Functions Virtualization / Software Defined Network periphery
  - New draft GS NFV 004 V0.0.4 (2014-Mar) includes LI forensics
- Structured expressions for capturing and exchanging forensics for a broad array of compliance needs
- Standard interfaces for requesting and delivering forensics
- Recognition of multiple forensics needs
  - Forensics performed on cloud-based services/systems
  - Virtual forensics tools in cloud for use on cloud and non-cloud services
- Support for unique LI/RD needs
- Cloud forensic specifications for compliance service providers
- Leveraging cybersecurity tools for forensic purposes
Cybersecurity tools (STIX) applied to cloud forensics

- Analyzing a compliance requisition
  - Case Intelligence
  - Courses of action and context

- Specifying an actor pattern
  - Patterns
  - Analyst

- Managing requisition response activities
  - Detection
  - Observable Acquisition
  - Case Intelligence
  - Operations
  - Patterns

- Sharing case intelligence
  - Decision Maker

Provider Organizations

Compliance Body

UC1 UC2 UC3 UC4