Holes in the Cloud

Weaknesses in Applying Digital Forensic Processes to Cloud Computing

Cloud computing is an expanding field with wide reaching applications. The qualities that make it so attractive to users and providers, it's multi-tenancy and distributed nature, also make it difficult to apply standard digital forensic practices within. This paper is concerned with identifying the most imminent legal and practical concerns in the application of forensics on cloud computing systems, highlighting current case law pertaining to the practice of cloud-related forensics, and offering suggestions which could lead to the development of normative or legislative remedies to the difficulties in applying digital forensics to cloud computing.

Digital Forensic Process

1. Search authority. In a legal investigation, legal authority is required to conduct a search or seizure of data.

2. Chain of custody. In legal contexts, chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct.

3. Imaging/hashing function. When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.

4. Validated tools. When possible, tools used for forensics should be validated to ensure reliability and correctness.

5. Analysis. Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.

6. Repeatability and reproducibility (quality assurance). The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts.

7. Reporting. The forensic analyst must document his or her analytical procedure and conclusions for use by others.

8. Possible presentation. In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience

Holes in the system

- DISTIBUTED DATA STORAGE
- NO BEST PRACTICES
- DECENTRALIZED AUTHROIZATION
- ISOLATION OF TARGETED EVIDENCE
- NO COMPLETE ROOT ACCESS
- INCOMPLETE LOGS
- SERVICE CONTRACTS LACK FORENSIC AWARENESS
- VOLITILE VM DATA

Forbes predicts that cloud computing will be a $500 billion industry by 2020

Proposed Cloud-Aware Forensic Process

iterative

1. Evidence Source, Identification and Preservation. Identifies target of investigation, gathers proper legal authorisation, prepare for preservation of possibly volatile artefacts.

2. Collection (chain of custody maintained). In legal contexts, chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct. When digital evidence is found, whenever possible it should be carefully duplicated and then hashed to validate the integrity of the copy.When possible,

3. Analysis. Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts. Tools used for forensics should be validated to ensure reliability and correctness.

4. Reporting/Presentation. The forensic analyst must document his or her analytical procedure and conclusions for use by others. In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience.

"By 2020, a corporate "no-cloud" policy will be as rare as a "no-internet" policy is today." -Gartner

Steps forward

Service contracts provide the quickest and simplest method of preventing future legal quandaries in cloud computing investigations. The development of an industry norm that contracts between providers and subscribers needs to be clear and exact in specifying ownership of information, jurisdictional particulars and avenues of access to structural and log information.

Third parties services with pre-set procedures for forensic investigations within major cloud providers to substantially decrease the range of extrajudicial cloud-computing services.

Regulatory norms set through legislation. While governmental control is not necessarily an effective tool and may present difficulty in maintaining relevance to a rapidly innovating field, legislation does offer the most profound method of ensuring legality in cloud-

In order to ensure trust in the judicial system's treatment of cloud computing related crimes, **a separate format for forensic investigation must be grown to deal with cloud computing's unique particularities,** one that can evolve and adapt in parallel to the industry. An iterative approach to cloud computing forensics that allows for multiple, simultaneous forensic processes to build upon each other has been suggested by the Information Assurance Research Group & Forensic Computing Lab in Australia. This approach would build upon the initial identification of evidence, creating a new process of forensic procedure when analysis dictates

A **revisal of MLAT procedures**, ensuring a smoother, quicker and less cumbersome result, is entirely necessary. In the short term, this can be addressed by creating an accelerated process within the the Office of International Affairs in the Department of Justice, training specific legal professionals to deal exclusively with MLA situations, and allocating more funding to these processes. In a long term, legislation of an entirely new process, streamlined to approve MLA requests from nations with similar forensic standards could serve a similar purpose in lessening the growing pressure on the Office of International Affairs in the Department of Justice that that the institution of the Visa Waiver System did in relation to U.S. Consular Offices.

Information	SaaS	PaaS	IaaS	Local
Networking	✗	✗	✗	✓
Storage	✗	✗	✗	✓
Servers	✗	✗	✗	✓
Virtualization	✗	✗	✗	✓
OS	✗	✗	✓	✓
Middleware	✗	✗	✓	✓
Runtime	✗	✗	✓	✓
Data	✗	✓	✓	✓
Application	✗	✓	✓	✓
Access Control	✓	✓	✓	✓

Information gaps available to investigators in different cloud service models

CASE LAW

Article 18 § 2703

Microsoft v. United States

In the course of a drug investigation the government sought the contents of an cloud-based Microsoft email account through a § 2703 warrant. The actual emails were stored on a Microsoft data server located in Ireland. The Second Circuit ruled that the actual conduct in this case fell outside U.S. jurisdiction, and thus, that the warrant was invalid.

United States v. Levin

Investigators tracking down users of a child pornography site (within a website platform) who obscured their physical location using anonymising software were denied a warrant to place surveillance software on the site which would identify users because the targets of the surveillance were not within the jurisdiction (or could not be assumed to be within the jurisdiction) of the magistrate to whom the warrant was presented

In Re Warrant to Search a Target Computer at Premises Unknown

Texas Judge denied a request from the FBI to install sophisticated surveillance software to track someone suspected of attempting to conduct a "sizeable wire transfer from [John Doe's] local bank [in Texas] to a foreign bank account." on the grounds that the warrant request was overbroad and too invasive and failed to meet the Fourth Amendment's requirement of "place to be searched, and the persons or things to be seized."

RULE 41