Case Study: Digital Forensics in the Cloud

Cloud computing offers immense opportunities for business and IT organizations by providing highly scalable infrastructure resources, pay-as-you-go service, and low-cost on-demand computing. While clouds attract diverse organizations, the security and trustworthiness of cloud infrastructure has become a rising concern. Clouds can be a target of attacks or can be used as a tool to launch attacks. Malicious individuals can easily exploit the power of cloud computing and can perform attacks from machines inside the cloud. Many of these attacks are novel and unique to clouds.

To illustrate the use of clouds for malicious purpose, we consider the following hypothetical scenario:

Bob is a successful businessman who runs a shopping website in the cloud. The site serves a number of customers every day and his organization makes a significant amount of profit from it. Therefore, if the site is down even for a few minutes, it will seriously hamper not only their profit but also the goodwill.

Mallory, a malicious attacker, decided to attack Bob's shopping website. She rented some machines in a cloud and launched a Distributed Denial of Service (DoS) attack to the shopping website using those rented machines. As a result, the site was down for an hour, which had quite a negative impact on Bob's business.

Consequently, Bob asked a forensic investigator to investigate the case. The investigator found that Bob's website records each visiting customer's IP address. Analyzing the visiting customer records, the investigator found that Bob's website was flooded by some IP addresses which are owned by a cloud service provider (CSP). Eventually, the investigator issued a subpoena to the corresponding cloud provider to provide him the network logs for those particular IP addresses.

On the other hand, Mallory managed to collude with the cloud provider after the attack. Therefore, while providing the logs to the investigator, the cloud provider supplied a tampered log to the investigator, who had no way to verify the correctness of the logs. Under this circumstance, Mallory will remain undetected.

We can see from this Case Study that there are various issues in the process of cloud forensics:

- A malicious user can also fraudulently claim that his/her instance was compromised by someone else who had launched a malicious activity. In the absence of any evidence, it will be difficult to prove his/her claim as false via a forensic investigation.
- Trust must be placed in the CSP to provide the correct information such a network logs and access times.
- As the storage system is no longer local, law enforcement agents cannot confiscate the suspect's computer and get access to the digital evidence even with a subpoena. There is no physical access as it is usually unfeasible to pin point the exact location of the data.

- In a cloud, each server contains files from many users. Hence, it is not feasible to seize servers from a data center without violating the privacy of many other benign users.
- Moreover, even if the data belonging to a particular suspect is identified, separating it from other users' data is difficult.
- In traditional computer forensics, investigators have full control over the evidence (e.g., router logs, process logs, and hard disks). Unfortunately, in a cloud, the control over data varies in different service models and service level agreements (SLA).
- If there is not persistent storage to VMs, turning off or rebooting a VM will eventually lose all the data residing in that VM.

Chain of Custody in the Cloud

Chain of custody is one of the most vital issues in traditional digital forensic investigation. Chain of custody should clearly depict how the evidence was collected, analyzed, and preserved in order to be presented as admissible evidence in court.

In a traditional forensic procedure, it is trivial to maintain an access history of time, location, and person to access the computer, hard disk, etc. of a suspect. On the other hand, in a cloud, we do not even know where a VM is physically located.

The Investigator's location and a VM's physical location can be in different time zones. Hence, maintaining a proper chain of custody is challenging in cloud forensics.

Excerpted from: Digital Forensics in the Cloud, Authors: Shams Zawoad and Ragib Hasan, University of Alabama at Birmingham, 2013