Towards a Systematic Analysis of Challenges and Issues in Secure Mobile Cloud Forensics

Shams Zawoad and Ragib Hasan
{zawoad, ragib}@cis.uab.edu
University of Alabama at Birmingham
Birmingham, Alabama 35294-1170, USA

***Abstract*—Though mobile cloud computing has become popular to mitigate the problem of low computing and storage resources of mobile devices, this has also brought new security challenges especially in the case of digital forensics. In this paper, we systematically analyze the mobile cloud forensics problem and explore the challenges and issues of this new branch of digital forensics. We also identify the requirements and propose a model to support reliable forensic investigations in the mobile cloud.**

***Keywords*—Mobile Cloud Forensics, Forensic Investigation**

I. Introduction

Leveraging the computing and storage resources provided by the cloud has become an effective way to solve the problem of resource constraints of mobile devices and has introduced the mobile cloud computing paradigm. By 2015, more than 2.4 billion users will use mobile devices to access the cloud computing services [1]. However, the recent iCloud hacking incident [2] shows that this model can also be a target of attackers. Deploying a botnet using mobile devices is also feasible [3]. To investigate these types of criminal activities, we need to execute digital forensics procedures in the mobile cloud environment to determine the facts about such malicious incidents, which we refer as *mobile cloud forensics*. We present a hypothetical case below (illustrated in Figure 1), where a mobile cloud has been used by a malware and we need to execute a digital forensics investigation to find out the facts.

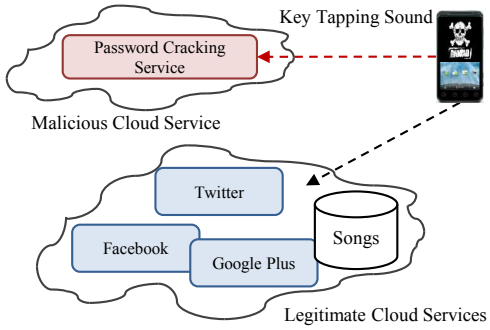

Fig. 1: Malicious usage of mobile cloud computing

MPlay is an online music player application for mobile devices, where users can listen to songs based on their choices. MPlay is also connected to Facebook, Twitter, and Google plus so that users can share what they like with their friends. However, this apparently safe looking application has an embedded malware, which records the key tapping sounds when a user tries to login to a social media. It sends the recorded sound to a cloud server to decode the password of these social media from the recorded sound. Alice, a user of MPlay lost her Google password and become a victim of identify fraud. Forensics investigators cannot prove that MPlay is behind this password hacking since they cannot access the cloud where the actual password cracking has occurred.

Unfortunately, many of the assumptions of traditional digital forensics are not valid in the mobile cloud environment. For example, investigators do not have physical access to the evidence that resides in clouds. Moreover, computing or storage resources are shared in the mobile cloud environment. The trustworthiness of the evidence can also be questionable since the court authority cannot verify the authenticity of the evidence collected from the cloud. As a result of these issues, mobile cloud forensics brings new challenges from both technical and legal point of view and has opened a new research area for security and forensics experts.

Contributions. In this paper, we systematically analyze the challenges and requirements to establish trustworthy forensics supports in the mobile cloud environment and propose a model to ensure reliable forensics in the mobile cloud. The requirements and the model can help researchers to focus on specific research sub-problems of the large mobile cloud forensics problem domain.

II. Challenges of Trustworthy Mobile Cloud Forensics

Shared Resources. When a user offloads a task from a mobile device to a cloud, many other users can offload their tasks to the same cloud at the same time. The computing resources can thus be shared between multiple users. Hence, it may happen that when one user is running a legitimate mobile cloud service, the same cloud is being used by a malware to meet its computing requirement. The same issue exists for storage services. For example, a single iCloud host can fulfill the storage requirements of hundreds of users, where one or a few of the users can store contraband documents in the shared storage. This resource sharing model in the mobile cloud brings two issues while executing digital forensics. When we acquire evidence from such an environment, first, we need to prove that evidence were not co-mingled with other users' data. And second, we need to preserve the privacy of other tenants while collecting evidence from the mobile cloud.

Forensics Data Acquisition. The established digital forensic procedures and tools assume that we have physical access to the computing resources, e.g., hard disk, network router, etc. Unfortunately, for mobile cloud forensics, we do not have the physical accessibility of the evidence, which are inside clouds. Hence, using existing tools and procedures, we cannot collect many crucial evidence, such as process logs, network logs, storage snapshot from the cloud.

Trustworthiness of Evidence Current mobile cloud infrastructures still do not provide full transparency or capabilities for the tracking and auditing of the file access history and data provenance. Since mobile cloud service provider (CSP) have full control over the data, they can always tamper with such evidence. Ensuring trustworthiness of evidence will become more challenging if a service provider colludes with a malicious user. A malicious user can collude with a CSP to remove all the traces of an illegal activity or the CSP can provide incomplete evidence to the investigator.

III. Requirements and a Conceptual Model for Forensics-enabled Mobile Cloud

A. Requirements

Secure Evidence Preservation. Because of the shared resources model, evidence should be preserved in such a way that while collecting evidence, it will not violate the privacy of honest users. Moreover, after preserving all the evidence, a mobile cloud service provider needs to ensure the integrity of the evidence. Without integrity preservation, the validity of the evidence will be questionable and the defense and the jury can object about it.

Secure Provenance. As provenance provides the history of an object, a mobile cloud provider can protect the chronological access history of evidence by implementing secure provenance. Secure provenance can be used to identify the root cause of some attacks and to identify attackers from the access history. By examining the provenance records, an investigator can identify when a cloud computing service was used by a legitimate application and when by a malware.

Availability of Evidence. Even if we preserve all the evidence securely, investigators will still depend on the mobile cloud providers to collect evidence. Mobile cloud service providers can play a vital role in this step by providing a web based management console or providing secure Application Programming Interface (API) to law enforcement agencies.

B. Conceptual Model

Based on the requirements, we argue that we need to focus on the cloud end of the mobile cloud infrastructures to support reliable forensics investigation in this environment. The proposed conceptual model for a forensics enabled mobile cloud is presented in Figure 2, which we discuss below.

Secure Evidence Preservation Module: This module will constantly monitor all the services provided by the cloud and store evidence securely in the evidence DB. Evidence can be network logs, registry logs, document access logs, etc. While preserving the data, this module can take care of segregating the data according to the mobile user to avoid commingling multiple users' data. This module will also preserve the confidentiality of the data from malicious cloud employee by using public-private key based encryption, so that only the law enforcement agencies can view the confidential evidence.

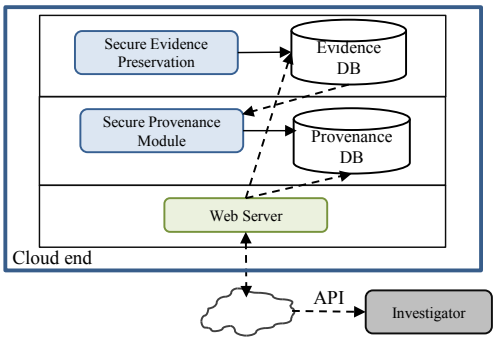

Fig. 2: A conceptual model for forensics-enabled mobile cloud

Secure Provenance Module: This module first generate the provenance records for file usage using the provenance aware file system (PASS) [4]. However, since provenance records are under the control of the CSP, they can always tamper with the provenance records. Hence, this module will apply secure provenance chaining approach [5] to preserve the integrity of the provenance records.

Access to Evidence Through API: We propose secure read-only Representational State Transfer (REST) APIs for the law enforcement agencies to collect the preserved evidence and the provenance information. A web server will communicate with the previously described modules to collect the requested data. To retrieve the required evidence, GET operations can be used with different query parameters.

IV. Conclusion

With the recent booming of mobile cloud computing, there is an increasing emphasis on providing trustworthy forensics supports in this environment. We need a collaborative attempt from public and private organizations as well as research and academia to overcome the challenges of mobile cloud forensics. By resolving the issues of mobile cloud forensics, we can open the opportunity of many new applications for the mobile devices and can help to secure this computing paradigm by ensuring reliable forensics investigations.

Acknowledgment

This research was supported by the National Science Foundation under the CAREER Award CNS-1351038.

References

[1] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *IEEE IWCMC*, 2013, pp. 655–659.

[2] theverge.com, "Hack leaks hundreds of nude celebrity photos," http://goo.gl/TaIfKb, 2014.

[3] C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, and Z. Tianning, "Andbot: towards advanced mobile botnets," in *USENIX LEET*, 2011, pp. 11–11.

[4] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in *USENIX ATC*, 2006, pp. 43–56.

[5] R. Hasan, R. Sion, and M. Winslett, "The case of the fake Picasso: Preventing history forgery with secure provenance," in *USENIX FAST*, 2009, pp. 1–12.