

Monitoring and detecting abnormal behavior in mobile cloud infrastructure

August 2012 [Network Operations and Management Symposium 2012](#)

Mobile Cloud Computing (MCC) is an emerging technology that leverages the benefits of cloud computing to enhance mobile computing capability. This paper discusses an example MCC service, in which mobile operating systems (OS) are virtualized in cloud infrastructure as mobile instances. These virtual mobile instances can run the same mobile applications as those supported by their counterparts on physical mobile devices. In this service, a given mobile device connects to a virtual mobile instance via a thin client and run applications on it. This way, users can execute mobile applications that demand computing resources that their mobile devices do not have. At the same time, it allows service providers to generate more profit from cloud computing business models.

Unfortunately, security is one of the major barriers to the adoption of MCC in the real world. In MCC, the security of a virtual mobile instance is as good as that of a ?real? mobile OS. However, a compromised virtual mobile instance represents a serious risk to the entire cloud infrastructure. For example, a malware that compromises a virtual mobile instance can then spread to all the other virtual machines on the same cloud infrastructure.

In this paper, we discuss how to identify and defeat security threats in MCC. Specifically, we discuss some possible security threats to MCC by way of illustrative service scenarios that involve both individual users and office staff. As a feasible solution of defeating the identified security threats, we propose a behavior-based abnormal detection methodology of monitoring both virtual hosts and network data. We show that our solution is better able to detect new, modified, and unknown abnormal activities than signature-based methods. The detection methodology is based on a machine learning technique, which uses both training (on normal and abnormal mobile applications) and monitoring real-time traffic. In our testing, our solution successfully detected the abnormal activities of malicious applications, which were intentionally injected into a mobile cloud test bed.

Title and author(s) of the original paper in IEEE Xplore:

Title: Monitoring and detecting abnormal behavior in mobile cloud infrastructure

Author: Taehyun Kim, Yeongrak Choi, Seunghee Han, Jae Yoon Chung, Jonghwan Hyun, Jian Li, and James Won-Ki Hong

This paper appears in: Network Operations and Management Symposium 2012

Issue Date: April 2012

[Back](#) [IEEE Xplore Version](#) [Similar Articles](#)

Source URL: <http://www.comsoc.org/ctn/monitoring-and-detecting-abnormal-behavior-mobile-cloud-infrastructure>