Journal of Network and Computer Applications 62 (2016) 171–184

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A new approach to mitigating security risks of phone clone co-location over mobile clouds

Seyed Yahya Vaezpour[a,*], Rui Zhang[b], Kui Wu[a], Jianping Wang[b], Gholamali C. Shoja[a]

[a] Computer Science Department, University of Victoria, BC, Canada
[b] Computer Science Department, City University of Hong Kong, Hong Kong

ARTICLE INFO

Article history:
Received 30 July 2015
Received in revised form
21 December 2015
Accepted 5 January 2016
Available online 18 January 2016

Keywords:
Mobile cloud
Phone clones
Security

ABSTRACT

Mobile cloud provides smart phone users with unprecedented opportunities to enjoy the abundant computing and storage resources of cloud computing. One viable scheme is to offload computational intensive applications to a mobile phone's agent in the cloud, which could be implemented as a thin virtual machine (VM), also termed as phone clone. Due to shared hardware components among co-resident VMs, a VM is subject to covert channel attacks and may potentially leak information to other VMs located in the same physical host. In this paper, we address two critical problems: how to allocate phone clones to minimize the risk of information leakage and how to migrate phone clones whenever the risk becomes higher than a given threshold. We design SWAP: a security aware provisioning and migration scheme for phone clones. Our solution utilizes the spatial and temporal features of phone clones, and by considering the online social connection of mobile users, we greatly simplify the search space of the optimal solution. Furthermore, we study the tradeoffs among security, cost, and load balancing in phone clone provisioning. We evaluate our solution using Reality Mining and Nodobo dataset. Experimental results indicate that our algorithms are nearly optimal for phone clone allocation and are effective in maintaining low security risk and minimizing the number of phone clone migrations.

Contents

* Corresponding author.
E-mail addresses: vaezpour@uvic.ca (S.Y. Vaezpour), zhangrui.ray@gmail.com (R. Zhang), wkui@uvic.ca (K. Wu), jianwang@cityu.edu.hk (J. Wang), gshoja@uvic.ca (G.C. Shoja).

http://dx.doi.org/10.1016/j.jnca.2016.01.005
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Telecom cloud refers to cloud computing services provided by telecom companies. Compared to third-party cloud service providers, telecom companies, particularly the mobile communication companies, have a unique advantage in the service provisioning: they provide the last-mile connection to users and thus have direct knowledge of users' activities. A telecom company can leverage the above advantages to provide its customers with high-quality and more attractive cloud computing services. One type of such services is to create phone clones within cloud computing to help mobile users augment the functionality of their smart phones and increase the lifetime of the battery.

The concept of phone clones (Chun et al., 2011) is to build software clones of smart phones on the cloud and enable mobile users to offload computation intensive tasks and backup data to the cloud. Current smartphone devices are normally installed with many useful applications to make users' daily life much easier and more efficient than before. Some applications, however, may require intensive calculation and consume a large amount of energy. In this case, the smartphone could offload the tasks to its clone in the cloud (Barbera et al., 2013a; Liu et al., 2013; Kosta et al., 2012).

Depending on different functionalities supported by the phone clones, they could be implemented as a process or a *thin* virtual machine (VM) (Chun et al., 2011; Kosta et al., 2012; Satyanarayanan et al., 2009) on a cloud host. Due to the ease of management and the richer functionalities of VM, we assume the VM version of phone clones in this paper. Figure 1 shows an example architecture of the system. To allow resource multiplexing, multiple VMs are usually allocated and managed with a hypervisor, such as KVM or Xen, in one physical machine. Due to the large number of mobile users, it is not surprising if one hypervisor hosts hundreds of phone clones. Under such circumstances, provisioning and migration strategies for phone clones become critical to the success of mobile telecom cloud.

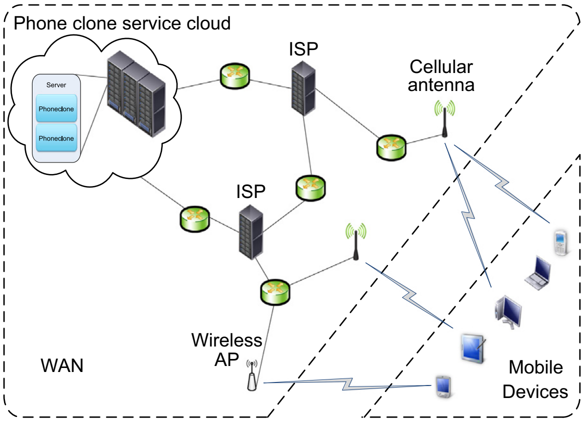

Fig. 1. System architecture of phone clones in mobile cloud.

We need to tackle two constraints in the allocation and migration of phone clones: security and resource. To give users' a reasonable sense of security, phone clones should be physically isolated. For example, users should feel more comfortable if their phone clones are co-located with those of their friends rather than strangers. Nevertheless, due to the limited number of physical hosts and the large number of mobile users, it may not be possible to find a good isolation for all phone clones. As a result, a phone clone may have to live together with other strangers' phone clones on the same host.

It has been shown that a VM can attack another VM on the same host via covert channel attacks (Ristenpart et al., 2009; Wu et al., 2012). Such attacks exploit the CPU cache or the memory bus in a virtualized environment to steal information from other VMs. It has been demonstrated in Ristenpart et al. (2009) and Wu et al. (2012) that covert channel can be effective and very hard to detect. The big challenge we are faced with in mobile cloud is: how to *mitigate* the risk of covert channel attacks when we do not have enough resource to physically isolate strangers' phone clones?

In this paper, we present our strategy to tackle this problem. We propose and evaluate SWAP: a s ecurity awa re p rovisioning and migration scheme for phone clones. For the provisioning of new phone clones, we take advantage of the mobile telecom cloud where it is easy to build a communication graph based on mobile users' communication history. The communication graph reflects the relationship between mobile users, and it should be safe to allocate together the phone clones that have a direct communication link, since they need to communicate anyway. Whenever this requirement cannot be met due to resource constraint, we then solve the optimization problem that minimizes the risk posed by potential covert channels. Our way of mitigating the negative impact of covert channels comes from the observation that covert channels normally need time to build (Gligor, 1993; Zhang et al., 2012). By constraining the co-locating time duration of two strangers' phone clones on the same host, we can counter the host limitation problem by migrating strategically selected VMs.

This paper makes the following contributions:

- First, we propose a system model that captures the mobile users' communication relationship and the potential risks when co-locating phone clones, and solve the optimization problem that minimizes the risks in the provisioning of new phone clones. The optimization problem requires intensive computations due to the large number of phone clones. To avoid this