Collaborative Monitoring of Moving Target Defense Mechanisms for Cloud Computing Dr. Sajjan G. Shiva

sshiva@memphis.edu (901) 678-5667

Professor, Computer Science Department

Director, Game Theory and Cyber Security Laboratory
(http://gtcs.cs.memphis.edu)

1. JUSTIFICATION

Cloud computing has become a prominent paradigm in recent years. It has gained popularity among the information technology (IT) world due to its ability to transfer the capital expenditure to operational expenditure [1]. The cloud consumer can get access to high-end computing infrastructure of clouds by only paying for the duration of usage. The other advantages of clouds are: On-demand self-service, broad network access, Resource pooling and rapid elasticity [2]. However, the cloud computing has also brought some vulnerabilities in addition to the existing security risks in traditional IT technology. This security concern responsibility is divided among the cloud users, the cloud vendors and the third party vendor involved in ensuring secure sensitive software or configurations. If the application level security is the responsibility of the cloud user, then the provider is responsible for the physical security and also for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator. In this proposal, we mainly focus on the security measures that are taken by the service providers to ensure the customers' data and application security and service availability.

Live migration of virtual machines (VM) is the process of moving virtual machines from one physical machine to another without any impact on virtual machine availability to users. The main purposes of live migration include: 1) Load balancing: In networked environment, if any server machine is becoming overloaded with virtual machines, then some of the virtual machines can be migrated from it to reduce the load. 2) Maintenance: If any maintenance activity is required in the physical machine which demands down time (e.g. Operating System upgrade, network configuration changes etc.) then, the existing virtual machines running on that machine could be moved to another physical machine and thus it can ensure the availability of those virtual machine to users. 3) Power Management: If some of the physical machines are being underutilized, then the virtual machines running on them could be live migrated to another machines and the previous machines could be shut down to reduce power consumption. 4) Fault

Tolerance: if at any point of time, the server starts malfunctioning, the running virtual machines can be migrated to another machine and the dysfunctional server can be investigated to find the reason of its misbehavior. In this way, the users of those virtual machines remain unaffected.

Live migration can be utilized in developing a moving target defense (MTD) environment, wherein the movement of resources creates additional burden on hackers to pierce the system. Live migration itself is not secure enough in cloud computing environment. Duncan et al. [4] have identified migration attack performed by the insider attacker as a very real threat to the security and integrity of customers' data. However, if live migration is performed in a trusted secured environment, it could be considered as a moving target defense strategy against several types of attacks. But, the migration aspects themselves expose the system and open up system boundaries providing the hacker additional opportunities to compromise the system. The vulnerabilities introduced by migration are reviewed in the next Section.

We propose the utilization of real-time monitors (programs that monitor appropriate, critical aspects of the application modules during their execution) at various levels of the system to detect and prevent hacking. The results of the proposed research would be useful for both cloud system providers and cloud system users to enhance and implement adequate security measures.