Title: Autonomic resilient cloud services using moving target defense
Author: Fargo Farah, University of Arizona

Abstract
Cloud Computing is a popular paradigm that aims at delivering computing as a utility. For the cloud computing paradigm to be fully adopted and effectively used, it is critical that the security mechanisms are robust and resilient to faults and attacks. DDoS attacks reaching 20Gbps, hacked system accounts by exploiting OS vulnerabilities, data confidentiality issues due to cloud breaches, etc. show the importance and requirement of the security for this paradigm. On the other hand, securing cloud systems is extremely complex due to the many interdependent tasks such as application layer firewalls, alert monitoring and analysis, source code analysis, and user identity management (especially with exabytes of IP traffic worldwide). It is strongly believed that we cannot build cloud services that are immune to attacks. Therefore, resiliency to attacks is becoming an important approach to address cyberattacks and mitigate their impacts. In our work, we present a methodology to develop an Autonomic Resilient Cloud Management (ARCM) based on Moving Target Defense (MTD), cloud service Behavior Obfuscation (BO), and Autonomic Computing. By continuously and randomly changing the cloud execution environments and the types of platforms used to run them, it will be extremely difficult for attackers to figure out the current execution environment and their existing vulnerabilities, thus allowing the system to evade attacks. We show how to apply the ARCM to one class of applications, MapReduce, and evaluate its performance and overhead.