Moving Target Defense in Distributed Systems

Syed Umer Bukhari, Doctoral Student,
Chalmers University of Technology, Sweden
syedu@chalmers.se

Abstract: Cloud computing has recently become increasingly popular. Additionally, a new model of cloud computing has emerged where cloud resources are being placed at the edge of the network closer to the user to reduce latency and improve real-time data processing. Nonetheless, both cloud and edge systems share many common security concerns. Typical defenses could include many of the traditional security mechanisms, such as firewalls, intrusion detection systems, anti-virus software, and encryption. However, these security measures are not always sufficient.

To enhance security, I explore the application of "moving target defense" techniques to fortify the system's defenses. The basic idea is to randomly move the target application between different edge or cloud nodes, while maintaining QoS guarantees akin to frequency hopping in communication systems. It helps to defend against physical attacks on the hardware and man-in-the-middle attacks as it moves the resource, which creates confusion for an attacker trying to fingerprint the target. There are many existing Moving Target Defense strategies, such as IP Shuffling, application shuffling. However, these strategies pose significant challenges, primarily due to the high cost of migrations and resource management. In my work, I investigate benefits and trade-offs of these different strategies from a system-perspective, to understand their potential benefits to security and their potential costs to the overall system and the critical application in particular.

Keywords: Moving Target Defense (MTD), Cloud, Edge Computing