Title: Cloud Computing Security Automation Framework

Speaker: Cihan Tunc

Abstract: Cloud services have gained tremendous attention as a utility paradigm and have been deployed extensively across a wide range of fields. However, Cloud security is not catching up to the fast adoption of its services and remains one of the biggest challenges for Cloud Service Providers (CSPs) and Cloud Service Consumers (CSCs) from the industry, government, and academia. These institutions are increasingly faced with threats such as DoS/DDoS attacks, ransomware attacks, and data breaches that are affecting the confidentiality, integrity, and availability of the cloud system resources. In the current cloud systems, security requires manual translation of security requirements into controls. Such an approach can be for the most part labor intensive, tedious, and error-prone leading to inevitable misconfigurations rendering the system-at-hand vulnerable to misuse, either malicious or unintentional. Therefore, it is of utmost importance to automate the configuration of the cloud systems per the client's security requirements steering clear from the caveats of the manual approach. Furthermore, cloud systems need to be continuously monitored for any misconfigurations. This paper presents a methodology allowing for cloud security automation and demonstrates how a cloud environment can be automatically configured to implement a set of NIST SP 800-53 security controls. In addition, this paper shows how the implementation of these controls in the cloud systems can be continuously monitored and validated.