Title: Cloud Computing and Security Anomaly Behavior Analysis (ABA) of Cyber Systems, Applications, and Protocols

Speaker: Salim Hariri, University of Arizona

Abstract: Cloud Computing is emerging as a new 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 malicious faults and attacks. Security in cloud computing is of major concern and a challenging research problem since it involves many interdependent tasks including application layer firewalls, configuration management, alert monitoring and analysis, source code analysis, and user identity management. It is widely accepted that we cannot build software and computing systems that are free from vulnerabilities and cannot be penetrated or attacked. In this presentation, I give an overview of University Arizona Anomaly Behavior Analysis (ABA) methodology that can be used to detect accurately any cyber-attacks against computers, networks, and applications. Our anomaly analysis approach utilizes feature selection, data mining, data analytics and statistical techniques to identify accurately the anomalous events that can be injected in files, networks, computers, and applications. We show as an example, how our approach has been validated on more than 10,000 files and showed that our approach can detect malicious HTML files with a true positive rate of 99% and a false positive rate of 0.8% for abnormal files.