Abstract: In this tutoria, we give an overview of an Anomaly Behavior Analysis (ABA) methodology that has successfully been used to analyze the behavior of different network protocols (IP, TCP, UDP), wireless networks, and ModBus protocols. We also show how to use this methodology to analyze the operations of the User-Cyber DNAs (UCD) data structures. The UCD-based behavior analysis uses statistical and data mining techniques to determine the current operating region of the application and also projects its behavior in the near future. The operating point (OP) of a user-cyber activities can be defined as a point in an n-dimensional space with respect to well-defined attributes. An acceptable operating zone for such behavior can be defined by combining the normal operating values for each attribute. At runtime, the operating point of a user behavior moves from one zone to another and that point might move to a region where the user behavior does not meet its security requirements. By continuously monitoring the operating point of a user behavior and using statistical and data mining techniques to project the trend of the operating point in the near future, we can then proactively predict and detect the anomalous behaviors that might have been caused by malicious attacks. We will show also how to apply this methodology to analyze DNS, WiFI, and HTTP protocols as well as how to detect malcious HTML files.

Bio: Salim Hariri is a Professor in the Department of Electrical and Computer Engineering at The University of Arizona. He received his Ph.D. in computer engineering from University of Southern California in 1986, and an MSc from The Ohio State University in 1982. He is the UA site director of NSF Center for Cloud and Autonomic Computing and he is the Editor-In-Chief for the CLUSTER COMPUTING JOURNAL (Springer, http://clus.edmgr.com) that presents research techniques and results in the area of high speed networks, parallel and distributed computing, software tools, and network-centric applications. He is the Founder of the IEEE/ACM International Symposium on High Performance Distributed Computing (HPDC) and the co-founder of the IEEE/ACM International Conference on Cloud and Autonomic Computing. He is co-author/editor of four books on Autonomic computing, parallel and distributed computing: Autonomic Computing,: Concepts, Infrastructure, and Applications (CRC Press, 2007), Tools and Environments for Parallel and Distributed Computing (Wiley, 2004), Virtual Computing: Concept, Design and Evaluation (Kluwer, 2001), and Active Middleware Services (Kluwer, 2000). His research interests include autonomic cyber security, big data analytics, resilient cloud services, critical infrastructure protections, and autonomic programming, and resilient Dynamic Data Driven Application Systems (rDDDAS).