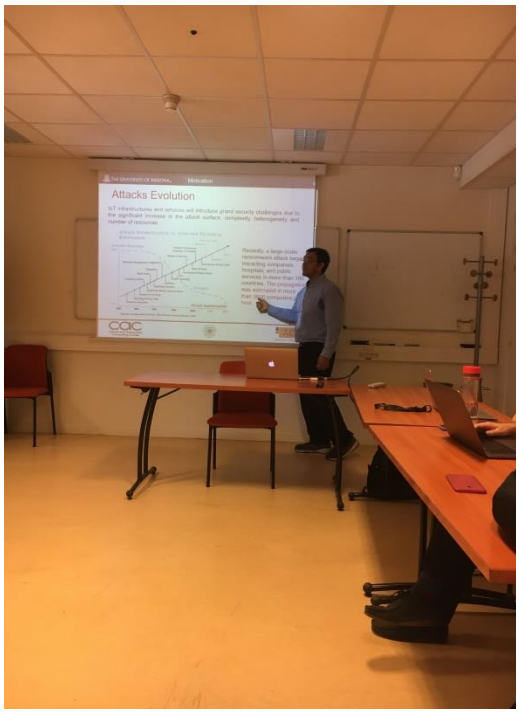
Title: An Anomaly Behavior Analysis Methodology for the Internet of Things



Speaker: Jesus Pacheco and Salim Hariri, University of Arizona

Abstract: Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services will lead to the development of the Internet of Things (IoT). The IoT services will be a key enabling technology to the development of smart infrastructures that will revolutionize the way we do business, manage critical services, and how we secure, protect, and entertain ourselves. However, with the use of IoT, we are experiencing grand challenges to secure and protect such advanced information services due to the significant increase in the attack surface. The interconnections between a growing number of devices expose the vulnerability of IoT applications to attackers. The security challenge consists of identifying accurately IoT devices, promptly detect vulnerabilities and exploitations of IoT devices, and stop or mitigate the impact of cyberattacks. In this work we aim at formalizing a general methodology to perform anomaly behavior analysis for IoT. We first introduce our IoT architecture for smart infrastructures that consists of four layers: end nodes (devices), communications, services, and application. We then show our multilayer IoT security framework and IoT architecture that consists of five planes: function specification or model plane, attack surface plane, impact plane, mitigation plane, and priority plane. Finally, we present a methodology to develop a general threat model in order to recognize the vulnerabilities in each layer and the possible countermeasures that can be deployed to mitigate their exploitation. In this scope, we show how to develop and deploy an anomaly behavior analysis based intrusion detection system (ABA-IDS) to detect anomalies that might be triggered by attacks against devices, protocols, information or services in our IoT framework.