Towards Secure, Privacy-Preserving, and Energy-Efficient Smart Parking Systems

The Oakland University and School of Engineering and Computer Science communities are invited to attend Ali Alqazzaz's defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.

Towards Secure, Privacy-Preserving, and Energy-Efficient Smart Parking Systems

Committee: Mohamed Zohdy, Ph.D. (Chair), Hua Ming, Ph.D. (Co-Chair), Richard Olawoyin, Ph.D., Dan Steffy, Ph.D.

Time: **10:00 – 12:00 p.m.**
Date: **Monday, March 11, 2019**
Location: **347 EC**

In this thesis, we first design a secure, energy-efficient, and privacy-preserving framework for smart parking systems. The framework relies on the publish/subscribe communication model for exchanging a huge volume of data with a large number of clients. On one hand, it provides functional services, including parking vacancy detection, real-time information for drivers about parking availability, driver guidance, and parking reservation. On the other hand, it provides security services at both the network and application layers. It supports mutual authentication using Elliptic Curve Cryptography-based certificates to ensure device/data authenticity, and provide security protection for users. This makes our framework secure against various types of cyber attacks, such as replay, phishing, and man-in-the-middle attacks. Second, we developed a testbed that is able to simulate large scale IoT deployments. Third, we implemented our system based on the constructed testbed to verify its effectiveness. The measurements obtained in our extensive tests indicate that using our framework get power consumption reduction of up to 58%, and the CPU utilization is reduced by 54.55%.

In addition, to ensure that the certificate validation process is done properly, we designed an automated tool to verify the TLS X.509 certificate validation process in real-world Message Queuing Telemetry Transport (MQTT) client applications. Our tool was used to analyze the broker's X.509 certificate validation in 15 well-known MQTT client applications. Our findings revealed that 33.3% of the examined applications are vulnerable to man-in-the-middle (MITM) and/or TLS renegotiation attacks.