UCF DEPARTMENT OF COMPUTER SCIENCE

Fall 2017 Distinguished Speaker Series

HACKING SENSORS

WEDNESDAY, OCTOBER 25, 2017

2:00 PM – HEC 450

Sensors are designed to measure sensor inputs (e.g., physical quantities) and transfer sensor outputs (e.g. voltage signal) into the embedded devices. In addition, sensor-equipped embedded systems (called sensing-and-actuation systems) decide their actuations according to these sensor outputs, and the systems have no doubt whether the sensor outputs are legitimate or not. Sensors are essential components for safety-critical systems such as self-driving cars, drones and medical devices. Breaking safety in these systems may cause loss of life or disasters. Because of these safety reasons, sensors are often designed to be robust against failure or faults. However, can they maintain safety under adversarial conditions? In this talk, I detail how sensors can be spoofed or prevented from providing correct operation through regular and side-channels. Attacks on various devices such as medical devices, drones, and self-driving cars will be shown. I'll complete the talk with a few directions and guides to prevent these attacks with a few open problems.

DR. YONGDAE KIM

Korea Advanced Institute of Science and Technology

Yongdae Kim is a Professor in the Department of Electrical Engineering and an affiliate professor in the Graduate School of Information Security at KAIST. He received PhD degree from the computer science department at the University of Southern California. Between 2002 and 2012, he was an associate/assistant professor in the Department of Computer Science and Engineering at the University of Minnesota - Twin Cities. Before joining U of Minnesota, he worked as a research staff for two years in Sconce Group in UC Irvine. Before coming to the US, he worked 6 years in ETRI for securing Korean cyber-infrastructure. Between 2013 and 2016, he served as a KAIST Chair Professor. He received NSF career award on storage security and McKnight Land-Grant Professorship Award from University of Minnesota in 2005. Currently, he is serving as a steering committee member of NDSS, an associate editor for ACM TISSEC, a PC chair for AsiaCCS 2018. His current research interests include security issues for various systems such as cyber physical systems, social networks, cellular networks, P2P systems, medical devices, storage systems, mobile/ad hoc/sensor networks, and anonymous communication systems.

Hosted by: Dr. Aziz Mohaisen

UCF

4328 Scorpius Street Room 346 Orlando, FL 32816

WWW.CS.UCF.EDU