**COLLOQUIUM**

Department of Computer Science and Engineering

University of South Carolina

**Securing Critical Infrastructure and Devices in the Internet of Things and Cyber-Physical Systems Era**

**Selcuk Uluagac**

Date: **March 27, 2017**

Time: **10:30-11:30am**

Place: **Swearingen 1A03 (Faculty Lounge)**

# Abstract

Cyber space is expanding fast with the introduction of new Internet of Things (IoT) and CPS devices. Wearables, smart watches, glasses, fitness trackers, medical devices, Internet-connected house appliances and vehicles have grown exponentially in a short period of time. Our everyday lives will be dominated by billions of connected smart devices by the end of this decade. Similarly, our nation's critical infrastructure (e.g., Smart Grid) also deploys a myriad of CPS and IoT equipment. Given the increasingly critical nature of the cyberspace of these CPS and IoT devices and the CPS infrastructure, it is imperative that they are secured against malicious activities. In this talk, I will briefly introduce three different current research topics related to the security of CPS and IoT devices and the CPS infrastructure: (1) The first topic will introduce the sensory channel threats to CPS and IoT systems. I will discuss how using sensory channels (e.g., light, temperature, infrared), an adversary can successfully attack IoT/CPS applications and devices. (2) The second topic will introduce the design of a novel IoT device fingerprinting and identification framework (IFF) to complement existing security solutions (e.g., authentication and access control) in identifying CPS and IoT devices (i.e., ensuring the devices are actually who they are). Finally, (3) The third topic will focus on the threat of counterfeit smart grid devices (e.g., PMUs, IEDs). Such devices with corrupted hardware components may exist in the deployment region without a priori knowledge and may leak important information to malicious entities.

**Dr. Selcuk Uluagac** is currently an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at Florida International University (FIU). Before joining FIU, he was a Senior Research Engineer in the School of Electrical and Computer Engineering (ECE) at Georgia Institute of Technology. Prior to Georgia Tech, he was a Senior Research Engineer at Symantec. He earned his Ph.D. with a concentration in information security and networking from the School of ECE, Georgia Tech in 2010. He also received an M.Sc. in Information Security from the School of Computer Science, Georgia Tech and an M.Sc. in ECE from Carnegie Mellon University in 2009 and 2002, respectively. He obtained his BS in Computer Science and Engineering and BA in Naval Science from the Turkish Naval Academy in 1997. The focus of his research is on cyber security topics with an emphasis on its practical and applied aspects. He is interested in and currently working on problems pertinent to the security of Internet of Things and Cyber-Physical Systems. In 2015, he received a Faculty Early Career Development (CAREER) Award from the US National Science Foundation (NSF). In 2015, he was also selected to receive fellowship from the US Air Force Office of Sponsored Research (AFOSR)’s 2015 Summer Faculty Fellowship Program. In 2016, he received the Summer Faculty Fellowship from the University of Padova, Italy. In 2007, he received the “Outstanding ECE Graduate Teaching Assistant Award” from the School of ECE, Georgia Tech. He is an active member of IEEE (senior grade), ACM, USENIX, and ASEE and a regular contributor to national panels and leading journals and conferences in the field. Currently, he is the area editor of Elsevier Journal of Network and Computer Applications and serves on the editorial board of the IEEE Communication Surveys and Tutorials. More information can be obtained from: <http://web.eng.fiu.edu/selcuk>.