

**P**rofesseur Selcuk Uluagac de Florida International University Miami, FL, USA animera un séminaire intitulé :

## Security and Privacy of IoT Apps and Devices

**Mercredi 14 décembre 2022 à 15h00 à la salle FC2 à l'ENSIAS**



**Biography:** Dr. Uluagac is currently an Eminent Scholar Chaired Associate Professor in the Department of Electrical and Computer Engineering at FIU, where he leads the Cyber-Physical Systems Security Lab, with an additional courtesy appointment in the Knight Foundation School of Computing and Information Science. Before FIU, he was a Senior Research Engineer at Georgia Tech and Symantec. He holds a PhD from Georgia Tech and MS from Carnegie Mellon University. In 2015, Dr. Uluagac received a Faculty Early Career Development (CAREER) Award from the US National Science Foundation (NSF), which is NSF's most prestigious award in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations. In 2015, he was awarded the US Air Force Office of Sponsored Research (AFOSR)'s Summer Faculty Fellowship.

In 2016, he received the Faculty Fellowship from the University of Padova, Italy. He has also received other awards for the quality of his mentoring and research, including (1) FIU Provost Office Top Scholar Award in Faculty with Notable Gains in Student Learning and Success (Sciences) Category, 2021, (2) FIU College of Engineering and Computing Faculty Award in Excellence in Research and Creative Activities Category, 2021, (3) FIU Eminent Scholar Chaired Associate Professor in the College of Engineering and Computing, 2020, In 2021, he received Google's ASPIRE Research award in security and privacy and received a fellowship from the Sapienza University of Rome, Italy in 2022.

**Abstract:** Cyber space is expanding fast with the introduction of new Internet of Things (IoT) and CPS devices. Wearables, smart watches, smart glasses, fitness trackers, medical devices, Internet-connected house appliances and vehicles have grown exponentially in a short period of time. Given the increasingly critical nature of the cyberspace of these IoT devices and applications, it is imperative that they are secured against malicious activities. In this talk, I will introduce different current research projects in Cyber-Physical Systems Security Lab (CSL) (<http://csl.fiu.edu>) related to the security and privacy of IoT devices and applications, highlighting how different machine learning algorithms enabled impeccable results: (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 to complement existing security solutions (e.g., authentication and access control) in identifying IoT devices (i.e., ensuring the devices are actually who they are). (3) The third topic will focus on how IoT devices deployed in smart settings (e.g., home, office) can leak sensitive information (events, activities) from different IoT apps and implementations even if the traffic is encrypted. (4) I will introduce a usable wearable-assisted continuous authentication framework where a wearable device (e.g., smartwatch) is used to authenticate a computer user continuously utilizing the motion sensors of the wearable. Finally, (5) I will share our most recent work in detecting illegal bitcoin operations (i.e., cryptojacking) that uses machine learning techniques to accurately detect the presence of unwarranted cryptomining activity in real-time.

