Department of Computer Science

Privacy and Security of Sensing in Cyber-physical Systems

Yan Long
University of Michigan

Hosted by Reza Curtmola

Date: Friday, February 9, 2024
Coffee: 10:45 AM – 11:00 AM
Time: 11:00 AM – 12:00 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m1800b872730a80901a9401ecfbedab89

Abstract:

Cyber-physical systems (CPS) such as mobile and wearable devices, Internet of Things, and autonomous vehicles are becoming ubiquitous in public and private spaces. While CPS depends on sensors to process physical information, the increasingly complex sensor hardware and the lack of low-level data protection and privacy controls create privacy and security challenges that are caused by the fundamental problem of sensor side channels. Such sensor side channels are challenging to prevent due to the undefined interactions between physical signals, sensor semiconductors, and downstream software.

Using the example of camera sensing, my talk explains how to characterize the causality, limits, and mitigations of sensor side channels through physics modeling and simulation. I will first explain how camera images can not only leak sensitive optical information, but also leak room audio unwittingly modulated in pixels. Then I will demonstrate how the electromagnetic leakage from smart home camera circuits allows eavesdroppers to reconstruct real-time, high-quality camera videos even through walls. Besides discussing my research vision of developing hardware-controlled and privacy-enhancing sensing mechanisms to protect future CPS from sensor side channels, I will also demonstrate the potential of utilizing these channels to enable novel multimodal sensing functionalities for enhancing the security of emerging technologies.

Bio:

Yan Long is a 5th-year Ph.D. candidate and Rackham Predoctoral Fellow in the EECS department at the University of Michigan, advised by Professor Kevin Fu and Professor Mingyan Liu. His research is mainly in the area of embedded systems security with a focus on protecting the security and privacy of analog and digital sensing in various forms of cyber-physical systems using hardware-software co-design. He also develops novel sensing systems to facilitate healthcare and security applications. His previous publications appeared at top international venues such as IEEE Security and Privacy, ACM CCS, NDSS, UbiComp, and SenSys.