香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

DEPARTMENT OF COMPUTER SCIENCE

SEMINAR

2025 SERIES

# Towards Secure, Reliable, and Efficient Cyber-Physical Systems (CPS): Attacks and Defenses

DATE & TIME

20 FEB 2025 (THU) 4:00 – 5:00 PM

VENUE

WLB 206, The Wing Lung Bank Building for Business Studies, Shaw Campus

## DR. TAO NI

Postdoctoral Researcher
Department of Computer Science
City University of Hong Kong

## ABSTRACT

Cyber-physical systems (CPS) such as mobile devices, Internet of Things (IoT), and autonomous vehicles are becoming ubiquitous in public and private spaces. While CPS integrate sensing, computation, control and networking into physical objects, the increasingly complex hardware and the lack of low-level data protection and privacy controls bring new security and privacy challenges resulting from side-channel information leakage and fundamental design flaws. Such side channels are challenging to prevent due to the undefined interactions between physical signals, sensor architectures, and wireless transmissions.

In this talk, I will systematically reveal the security and privacy in the key components of CPS in critical infrastructures by characterize the causality, limits, and mitigations of contactless side channels through physics modeling and computation. Specifically, I will introduce a series of my dissertation research of using hardware-software co-design and cutting-edge AI techniques to investigate side-channel attacks against smartphone embedded sensors, computation and control units in IoT devices, and metadata in wireless transmission, as well as proposing effective defense methods. Beyond highlighting the academic and industrial impact of these studies, I will also demonstrate my future research vision of developing software-defined, model-safe and privacy-preserving mechanisms to protect emerging CPS platforms.

SPEAKER'S BIOGRAPHY

REGISTER NOW

**Enquiries:** 3411-2385 **Email:** comp@comp.hkbu.edu.hk **Website:** https://bit.ly/bucs-events