



**THE CHINESE UNIVERSITY OF HONG KONG**  
Department of Information Engineering  
*Seminar*

**Electromagnetic Signal Injection Attacks on  
Embedded Systems - Modeling and Detection**  
**By**  
**Mr. ZHANG Youqian**  
**Department of Computer Science, University of Oxford**

**Date : 7 October 2022 (Friday)**

**Time : 11:00am to 12:00nn**

**Venue : Rm801, HSH Engineering Building, CUHK**

*Abstract*

Embedded systems are ubiquitous in our lives, from smart locks in home automation to robotic arms in industrial equipment, playing key roles in many safety- and security-critical applications. The embedded systems interact with the physical world through two essential interfaces: they use "sensors" to sense environmental changes and control "actuators" to cause physical impacts. In recent years, studies have demonstrated remotely manipulating sensor readings or actuator actions by electromagnetic interference (EMI). Such malicious manipulation can control the embedded systems as an attacker wishes, threatening users' privacy and safety, for example, unlocking a smart lock or raising the temperature of infant incubators.

Detecting such attacks is becoming increasingly essential, and this talk will cover two novel detection methods fitting various embedded systems regardless of their types. In addition to these detection methods, this talk also introduces a state-of-the-art attack to inject arbitrary messages into differential signaling technique, from which many protocols such as USB, Ethernet, and CAN bus derive their electromagnetic noise immunity.

*Biography*

Youqian Zhang is a DPhil candidate at the University of Oxford, supervised by Professor Kasper Rasmussen. Youqian's current research focuses on embedded system security, specifically using electromagnetic waves to manipulate crucial data in embedded systems and proposing novel detection and mitigation methods. He obtained his Master's and Bachelor's degrees from Imperial College London and Hong Kong Polytechnic University, respectively.

**\*\* ALL ARE WELCOME \*\***