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

2024 SERIES

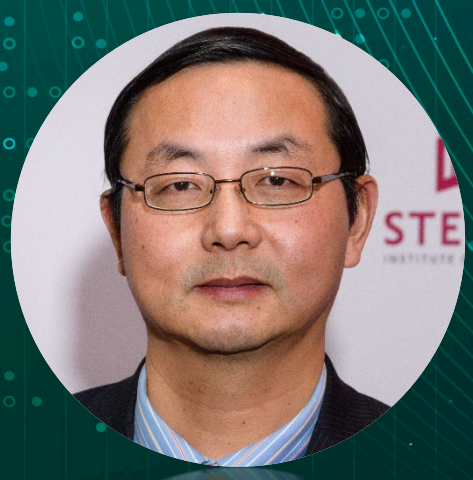
Seeing Is Believing: Extracting Semantic Information from Video for Verifying IoT Events

DATE & TIME

24 OCT 2024 (THU) 11:30 AM – 12:30 PM

VENUE

Mr. and Mrs. Lee Siu Lun Lecture Theatre (WLB205),
The Wing Lung Bank Building for Business Studies, Shaw Campus



PROF. XIAOJIANG DU

Anson Wood Burchard Endowed-Chair Professor
Department of Electrical and Computer Engineering
Stevens Institute of Technology

ABSTRACT

Along with the increasing popularity of smart home IoT devices, more users are turning to smart home automation platforms to control and automate their IoT devices. However, IoT automation is vulnerable to spoofed event attacks. Given that IoT devices are intricately linked with the physical environment and operate autonomously, event-based attacks can pose serious safety and security challenges. Our observations show that many IoT events are accompanied by visual modifications in objects such as shape alterations (for example, contact sensor events correspond with door movement) or changes in color/brightness (for example, a functioning microwave oven with the internal light switched on). These alterations can be detected by the commonly deployed smart cameras, providing a visually rich but challenging to manipulate channel for verifying IoT events. We introduce IoTSentry, the first system of its kind to extract high-level semantic information from streaming video data and pixels for IoT event verification. We have designed a Siamese deep neural network to identify variations in the appearance of IoT devices and interior objects. These are used as the yardstick for verifying IoT events received at IoT automation platforms. Upon assessing IoTSentry with 21 IoT devices (8 types), the results demonstrate that IoTSentry can be trained within 120 seconds, yielding an accuracy rate of over 96.7% in recognizing device states. We have deployed the 21 IoT devices and IoTSentry on two real-world smart home test sites. Over the course of our one-week evaluation, IoTSentry consistently achieved an average detection rate of 99.24% in identifying attack instances. Moreover, it triggered no more than 2 false alarms per day on each test site. This work has been published at one of the top wireless security conferences – ACM WiSec 2024.

SPEAKER'S BIOGRAPHY

REGISTER NOW

Enquiries: 3411-5935 **Email:** comp@comp.hkbu.edu.hk **Website:** https://bit.ly/bucs-events