In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Secret-Free Trust Initialization for Internet-of-Things Devices

by

Professor Ming LI

Department of Electrical and Computer Engineering

University of Arizona, USA

Date : 11th June, 2018 (Mon.)

Time : 2:00pm – 3:00pm

Venue : Room 1009, William M.W. Mong Engineering Building
The Chinese University of Hong Kong

Abstract

With the proliferation of personal wireless devices in the Internet-of-Things (IoT), such as mobile phones, wearable devices and smart home sensors, it becomes more and more critical to secure the communications among them by establishing initial trust (authenticated secret key establishment). The major challenge, is the lack of pre-shared secrets among IoT devices that are deployed in an ad hoc manner. In addition, personal devices are likely to be constrained in hardware interfaces and computational resources. Existing techniques such as device pairing usually need auxiliary secure channels or user interfaces that may not be present, and require significant human effort. In this talk, we take a different "in-band" approach to establish initial trust without prior secrets, which is done purely using the wireless channel and with little human support. The key idea is to assure message integrity protection and authentication by detecting or preventing signal manipulation (or man-in-the-middle) attacks in the wireless channel. We first present a game-theoretic approach or modeling and analysis of signal cancellation attacks, where the optimal strategy of the attacker and defender are derived. Then we present a channel-randomization based method to thwart signal cancellation attacks. When the channel is fully known by the adversary, we introduce several PHY-layer primitives for integrity protection, by either detecting signal cancellation attacks with a helper, or preventing simultaneous signal cancellation using multiple verifiers, and exploit helper movement for authentication. Our schemes can resolve important challenges in IoT trust establishment, by eliminating default passwords, the need of public key infrastructure, while satisfying the efficiency and scalability requirements. Finally, I will discuss some future research directions in this area.

Biography

Ming Li is an Associate Professor in the Department of Electrical and Computer Engineering of University of Arizona. He was an Assistant Professor in the Computer Science Department at Utah State University from 2011 to 2015. He received his Ph.D. in ECE from Worcester Polytechnic Institute in 2011. His main research interests are wireless and cyber security, with current emphases on cross-layer optimization and machine learning in wireless networks, security and privacy of the Internet-of-Things and dynamic spectrum sharing, privacy-preserving data analytics, and security in cyber-physical systems including autonomous vehicles. He has been on the editorial boards of IEEE Transactions on Wireless Communications, and IEEE Wireless Communications Letters. He received the NSF Early Faculty Development (CAREER) Award in 2014, and the ONR Young Investigator Program (YIP) Award in 2016. He has served as a TPC co-chair of the CISS symposium of International Conference on Communications (ICC) in 2018. He is a senior member of IEEE.

**** ALL ARE WELCOME ****

Host: Professor Sherman S. M. Chow (Tel: 3943- 8376, Email: smchow@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)