香港城市大學
City University of Hong Kong

Department of Computer Science

COMPUTER SCIENCE COLLOQUIUM

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

SPEAKER	**Prof LI Ming** Associate Professor Department of Electrical and Computer Engineering University of Arizona USA	DATE	14 June 2018 (Thursday)
		TIME	9:30 am - 10:30 am
		VENUE	CS Seminar Room, Y6405 6th Floor, Yellow Zone Yeung Kin Man Academic Building City University of Hong Kong 83 Tat Chee Avenue Kowloon Tong

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 HELP, which is a novel physical layer primitive that can detect any message modification with the aid of a co-located helper device that injects random authentication signals. HELP enables us to securely pair new devices with the hub with little extra effort. Then we introduce VERSE, another primitive that prevents signal manipulation using three or more devices as simultaneous verifiers, whose security is derived from basic signal propagation properties and geometrical constraints. VERSE enables secure pairing of a group of devices with the hub at the same time. Finally, we introduce the SFIRE protocol, which authenticates new devices with a moving helper based on received signal strength ratio, and can be implemented on commercial-off-the-shelf devices. 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.

Prof Li 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!

In case of questions, please contact Dr WANG Cong at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.