TEMPLE UNIVERSITY®

Spring 2021 Colloquium

Department of Computer and Information Sciences

Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks and Defense

Dr. Xinwen Fu

Professor
Department of Computer Science
University of Massachusetts Lowell

Thursday, Feb. 11th, 11 AM
Zoom Link: https://temple.zoom.us/j/4711287967

Abstract: This talk covers our research in the USENIX Security 2020 and INFOCOM 2020 papers. Our main contribution is the discovery of the insecurity of Bluetooth Low Energy one-way secure connections only (SCO) mode. In the SCO mode, a BLE device accepts only secure pairing such as Passkey Entry and Numeric Comparison from an initiator, e.g., an Android mobile. However, the BLE specification does not require the SCO mode for the initiator and does not specify how the BLE programming framework should implement this mode. We show that the BLE programming framework of the initiator must properly handle SCO initiation, status management, error handling, and bond management; otherwise, severe flaws can be exploited to perform downgrade attacks, forcing the BLE pairing protocols to run in an insecure mode without user's awareness. Due to such system flaws from the BLE programming framework, all BLE apps in Android are subject to our downgrade attacks. In addition to Android, we also find all major OSes including iOS, macOS, Windows, and Linux do not support the SCO mode properly. To defend against our attacks, we have built a prototype for the SCO mode on Android 8 atop Android OpenSource Project (AOSP). We also present an application-level defense measure.

Bio: Dr. Xinwen Fu is a professor in the Department of Computer Science, University of Massachusetts Lowell. He was a tenured Associate Professor at University of Central Florida. His current research interests are in computer and network security and privacy. Dr. Fu has published at the four top computer security conferences including Oakland, CCS, USENIX Security and NDSS, and prestigious journals such as ACM/IEEE Transactions on Networking (ToN) and IEEE Transactions on Dependable and Secure Computing (TDSC). He spoke at various technical security conferences including Black Hat.